(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5775174号
(P5775174)

(45)発行日　平成27年9月9日(2015.9.9)　(24)登録日　平成27年7月10日(2015.7.10)

(51)Int.Cl.		F I		
H04W 12/06	(2009.01)	H04W	12/06	
H04W 36/18	(2009.01)	H04W	36/18	
H04W 36/14	(2009.01)	H04W	36/14	
H04M 3/00	(2006.01)	H04M	3/00	C
H04M 3/42	(2006.01)	H04M	3/42	C

請求項の数 15　(全 51 頁)　最終頁に続く

(21)出願番号　特願2013-547709 (P2013-547709)
(86)(22)出願日　平成23年12月30日 (2011.12.30)
(65)公表番号　特表2014-506060 (P2014-506060A)
(43)公表日　平成26年3月6日 (2014.3.6)
(86)国際出願番号　PCT/US2011/068206
(87)国際公開番号　WO2012/092604
(87)国際公開日　平成24年7月5日 (2012.7.5)
審査請求日　平成25年9月2日 (2013.9.2)
(31)優先権主張番号　61/428,663
(32)優先日　平成22年12月30日 (2010.12.30)
(33)優先権主張国　米国(US)

(73)特許権者　510030995
インターデイジタル　パテント　ホールディングス　インコーポレイテッド
アメリカ合衆国　１９８０９　デラウェア州　ウィルミントン　ベルビュー　パークウェイ　２００　スイート　３００
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　ヨゲンドラ　シー．シャー
アメリカ合衆国　１９３４１　ペンシルベニア州　エクストン　リージェンシー　コート　１０

最終頁に続く

(54)【発明の名称】通信ハンドオフのシナリオのための認証およびセキュアチャネルの設定

(57)【特許請求の範囲】

【請求項１】

モバイル装置の認証で使用するための認証の認証情報を生成する方法であって、

前記モバイル装置と第１のアクセスネットワークとの間の持続的な通信層を介して、ネットワークサーバと前記モバイル装置との間で共有される持続的な通信層の認証情報を確立するステップであって、前記持続的な通信層の認証情報は、前記第１のアクセスネットワークを使用して前記ネットワークサーバからサービスを受けるために前記モバイル装置を前記持続的な通信層上で認証するように構成される、確立するステップと、

第２のアクセスネットワーク上のネットワーク通信エンティティを発見するステップであって、前記モバイル装置は前記第２のアクセスネットワークの通信層上で認証を行なうためおよび前記第２のアクセスネットワークを使用して前記ネットワークサーバから前記サービスを受けるために第２の通信層の認証情報を使用し、前記第２の通信層の認証情報は前記持続的な通信層の認証情報と異なる、発見するステップと、

前記持続的な通信層の認証情報に基づいて、前記第２の通信層の認証情報を生成するステップであって、前記第２の通信層の認証情報は前記第２のアクセスネットワークの前記通信層上で認証を行なうためのものであり、前記第２のアクセスネットワークにおける前記認証は、前記モバイル装置が前記第１のアクセスネットワークから前記第２のアクセスネットワークに切り替わることおよび前記第２のアクセスネットワークを使用して前記ネットワークサーバから前記サービスを受けることを可能にし、前記持続的な通信層の認証情報は前記第１のアクセスネットワークから前記第２のアクセスネットワークへの前記切

り替え後も存続する、生成するステップと
を含むことを特徴とする方法。
【請求項２】
前記持続的な通信層はアプリケーション層を含み、前記持続的な通信層の認証情報はアプリケーション層の認証情報を含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記ネットワーク通信エンティティと前記第２のアクセスネットワークのアプリケーション層で通信するためのアプリケーション層識別を決定するステップと、
前記ネットワーク通信エンティティと前記第２のアクセスネットワークのアクセス層で通信するためのアクセス層識別を前記アプリケーション層識別から決定するステップと、
前記アクセス層識別を前記第２のアクセスネットワークの前記ネットワーク通信エンティティに送信して、前記第２の通信層の認証情報の生成を開始するステップと
をさらに含むことを特徴とする請求項２に記載の方法。
【請求項４】
前記モバイル装置は、前記第２の通信層の認証情報を前記アプリケーション層から前記第２のアクセスネットワークの前記通信層に通信するように構成されることを特徴とする請求項２に記載の方法。
【請求項５】
前記第２の通信層の認証情報は、鍵導出機能を使用して前記アプリケーション層の認証情報から生成されることを特徴とする請求項２に記載の方法。
【請求項６】
前記第２のアクセスネットワークの前記通信層は前記第２のアクセスネットワークのアクセス層を含み、前記第２の通信層の認証情報はアクセス層の認証情報であることを特徴とする請求項１に記載の方法。
【請求項７】
前記アクセス層の認証情報はセッション鍵を含むことを特徴とする請求項６に記載の方法。
【請求項８】
別のアクセス層の認証情報を使用して、前記第１のアクセスネットワーク上で前記モバイル装置を認証するステップをさらに含むことを特徴とする請求項６に記載の方法。
【請求項９】
前記持続的な通信層の認証情報は、前記第１のアクセスネットワークのアクセス層上で前記モバイル装置を認証するために使用される前記アクセス層の認証情報を使用して確立されることを特徴とする請求項８に記載の方法。
【請求項１０】
前記第１のアクセスネットワークはセルラ通信ネットワークであり、前記第２のアクセスネットワークはワイヤレスローカルエリアネットワーク（ＷＬＡＮ）であることを特徴とする請求項１に記載の方法。
【請求項１１】
前記方法は通信層のハンドオフ中に行われることを特徴とする請求項１に記載の方法。
【請求項１２】
前記ネットワーク通信エンティティはアクセスポイント（ＡＰ）またはホットスポットを含み、前記ネットワークサーバは、認証、認可および課金（ＡＡＡ）サーバ、ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）ゲートウェイ、またはＷＬＡＮアクセスポイント（ＡＰ）を含むことを特徴とする請求項１に記載の方法。
【請求項１３】
前記ＡＡＡサーバはＯｐｅｎＩＤプロバイダ（ＯＰ）サーバを含み、前記ＷＬＡＮゲートウェイおよび前記ＷＬＡＮ　ＡＰはリライングパーティ（ＲＰ）を含むことを特徴とする請求項１２に記載の方法。
【請求項１４】

前記ＯＰは、モバイルネットワーク事業者（ＭＮＯ）または前記ＭＮＯに関連付けられたアプリケーションサービスプロバイダ（ＡＳＰ）を含むことを特徴とする請求項１３に記載の方法。

【請求項１５】

前記第２の通信層の認証情報はローカルＯｐｅｎＩＤプロバイダ（ＯＰ）にて生成されることを特徴とする請求項１に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、無線通信に関する。

【背景技術】

【０００２】

（関連出願の相互参照）

本出願は、２０１０年１２月３０日に出願された米国仮特許出願第６１／４２８，６６３号の利益を主張し、同出願の内容は参照により全体が本明細書に取り込まれる。

【０００３】

ユーザは、一般に、ネットワーク間を移動しながら１つのサービスを継続して使用することができる。ユーザが、現在のネットワークによってサービスされている場所から、移動先ネットワークによってサービスされている場所に移動する時には、例えばアクセス層でハンドオフを行うことができる。ハンドオフが行われる時、ユーザは、移動しようとする場所にサービスしている移動先ネットワークに対して認証される必要がある場合がある。アクセス層における認証はハンドオフのたびに発生する可能性があり、ユーザ装置は、事前に供給された認証情報を使用してアクセス層で移動先ネットワークにアクセスすることができる。

【０００４】

ユーザの通信装置は、階層化された通信機構を使用して通信することができる。多くの場合、異なる層の通信はそれぞれ独自のセキュリティを必要とする。ハンドオフは、階層化されたネットワーク内の１つのノードと別のノードとの間で発生する場合がある。そのようなハンドオフを実現する技術は存在するが、通信は、現在使用されているセキュリティの関連付けまたは機構の中断を要する可能性がある。

【０００５】

一例によると、アクセス層のハンドオフでは、アクセス層で別のネットワークへのハンドオフが行われる時に追加的なセキュリティの確立を使用することにより、現在使用されているセキュリティ機構のそのような中断を生じさせる可能性がある。例えば、追加的なセキュリティの確立は、アクセス層でハンドオフが発生するたびに、認証および／またはセキュリティ鍵合意の別のセッションを含む場合がある。アクセス層のハンドオフはより頻繁になる可能性があり、アクセス層のハンドオフが発生するたびに追加的なセキュリティセッションを確立すると、遅延および／または不必要な無線通信および／またはネットワークの認証の基盤機構への負担を引き起こす可能性がある。その結果、シームレスなハンドオフを実現することが難しくなる可能性がある。

【発明の概要】

【０００６】

この概要は、以下の詳細な説明でさらに説明する様々な概念を簡略化した形態で紹介するために提供される。

【０００７】

ネットワークサーバのサービスにアクセスするためにモバイル装置を認証するための認証の認証情報をモバイル装置で生成するシステム、方法、および装置の実施形態が本明細書に記載される。１つの層における認証とそれに関連する認証情報の持続性を使用して、別の層で認証情報を確立することができる。本明細書に記載されるように、ネットワークサーバと共有される、持続的な通信層の認証情報を確立することができる。例えば、持続

的な通信層の認証情報は、アプリケーション層で生成されるアプリケーション層の認証情報、または１つのネットワークから別のネットワークへのハンドオフ後も存続する持続的な通信層で生成される他の認証情報とすることができる。持続的な通信層の認証情報は、第１のネットワークの持続的な通信層を介して確立することができる。持続的な通信層の認証情報は、その第１のネットワークを使用してネットワークサーバからサービスを受けるためにモバイル装置を認証するように構成される。第２のネットワーク上のネットワーク通信エンティティを発見することができ、持続的な通信層の認証情報に基づいて認証の認証情報を生成することができる。その認証の認証情報を使用して、持続的な通信層以外の通信層を介して第２のネットワークに対して認証して、モバイル装置が第２のネットワークを使用してネットワークサーバからサービスを受けられるようにすることができる。

【０００８】

別の例示的実施形態によると、通信ネットワーク上に存在するアプリケーションサーバでモバイル装置を認証する際に使用する認証の認証情報をアプリケーションサーバで得ることができる。例えば、アプリケーション層の認証情報から導出される認証の認証情報を得ることができる。認証の認証情報は、アプリケーションサーバに関連付けられたアプリケーション層を介して得ることができる。認証の認証情報は、アプリケーションサーバからのサービスにアクセスするためにモバイル通信装置を認証するように構成することができる。他の通信層でモバイル装置を認証するために、認証の認証情報をアプリケーション層から他の通信層に送信することができる。

【０００９】

例示的実施形態によると、他の通信層はアクセス層とすることができる。アクセス層は、物理層、データリンク層、および／またはネットワーク層である。他の通信層がアクセス層である場合は、認証の認証情報は、アクセス層での認証に使用されるアクセス層の認証情報とすることができる。

【００１０】

上記概要は、以下の詳細な説明でさらに説明する概念の抜粋を簡略化した形態で紹介するために提供される。この概要は、特許請求の範囲の主題の主要な特徴や必須の特徴を明らかにするものでも、特許請求の範囲の主題の範囲を限定するために使用されるものでもない。さらに、特許請求の範囲の主題は、本開示の任意の箇所に記述される不利点のいずれかまたはすべてを解決する制限事項にも限定されない。

【図面の簡単な説明】

【００１１】

添付図面との関連で例として与える以下の記述から、より詳細な理解が得られる。

【図１Ａ】１つまたは複数の開示される実施形態を実施することが可能な例示的通信システムのシステム図である。

【図１Ｂ】図１Ａに示す通信システム内で使用することが可能な例示的ワイヤレス送信／受信ユニット（ＷＴＲＵ）のシステム図である。

【図１Ｃ】図１Ａに示す通信システム内で使用することが可能な例示的無線アクセスネットワークおよび例示的コアネットワークのシステム図である。

【図２】アプリケーション層のセッションについてのハンドオフシナリオを説明する流れ図である。

【図３】アプリケーション層のセッションについての別のハンドオフシナリオを説明する流れ図である。

【図４Ａ】ローカルＯｐｅｎＩＤを使用したプロトコルの実現を説明する流れ図である。

【図４Ｂ】ローカルＯｐｅｎＩＤを使用したプロトコルの実現を説明する流れ図である。

【図５Ａ】ローカルＯｐｅｎＩＤを使用し、アクセス／権限を付与するプロトコルの実現を説明する流れ図である。

【図５Ｂ】ローカルＯｐｅｎＩＤを使用し、アクセス／権限を付与するプロトコルの実現を説明する流れ図である。

【図６】リライングパーティ（relying party）（ＲＰ）として機能する認証、認可およ

び課金（ＡＡＡ）サーバを用いる、ユニバーサルアクセス方法（ＵＡＭ）とＯｐｅｎＩＤとの統合を説明する流れ図である。
【図７】ＲＰとして機能するワイヤレスローカルエリアネットワーク（ＷＬＡＮ）ゲートウェイ（ＧＷ）を用いる、ＵＡＭとＯｐｅｎＩＤとの統合を説明する流れ図である。
【図８】ＲＰとして機能するＡＡＡサーバを用いる、拡張可能認証プロトコル（ＥＡＰ）とＯｐｅｎＩＤとの統合を説明する流れ図である。
【図９】ＲＰとして機能するＡＡＡサーバを用いる、ＥＡＰとＯｐｅｎＩＤとの統合を説明する流れ図である。
【図１０】ＲＰとして機能するＡＡＡサーバを用いるＥＡＰとＯｐｅｎＩＤとの統合、およびローカルＯｐｅｎＩＤプロバイダ（ローカルＯＰ）の実装を説明する流れ図である。
【図１１】ＲＰとして機能するＡＡＡサーバを用いる、ＥＡＰとＯｐｅｎＩＤとの統合を説明する別の流れ図である。
【図１２】ＡＡＡサーバをＯＰサーバとして実装する認証プロトコルを説明する流れ図である。
【図１３】ＥＡＰプロトコルメッセージへのＯｐｅｎＩＤメッセージの組み込みを説明する流れ図である。
【図１４】ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔを使用する、サービスのためのユーザ機器（ＵＥ）の認証を説明する流れ図である。
【図１５】ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔおよびローカルを使用する、サービスのためのＵＥの認証を説明する流れ図である。
【発明を実施するための形態】
【００１２】
本明細書には、例えばＯｐｅｎＩＤプロトコルなどの連携識別（federated identity）およびシングルサインオン（ＳＳＯ）を使用して、異種のネットワーク間のシームレスなユーザ／装置の認証とセキュアな移動性とを可能にするための各種実装が記載される。本明細書に記載される実施形態は、あるネットワークに対する認証情報を活用して、別のネットワークに対する認証を行うことができる。一例示的実施形態では、１つのネットワークの持続的な通信層で生成される持続的な通信層の認証情報を使用して逆ブートストラップを行い、別のネットワークで要求に応じてかつシームレスな方式でセキュリティ層の認証および／またはセキュアなトンネルの設定を完了することができる。例示的実施形態によると、持続的な通信層の認証情報は、アプリケーション層で生成されるアプリケーション層の認証情報、または１つのネットワークから別のネットワークへのハンドオフ後も存続する通信層で生成される別の認証情報である。本発明の実施形態では、ハンドオフのシナリオでアプリケーション層の認証情報を使用して別の層（例えば、非持続性の通信層）における認証を行うことを記載するが、持続的な通信層で確立され、ネットワーク間のハンドオフ後も存続する任意の他の認証情報が使用されてよいことは理解されよう。
【００１３】
一実施形態によると、ハンドオフ（例えばアクセス層のハンドオフ）時にモバイル装置の認証で使用するアクセス層の認証の認証情報を生成するシステムおよび方法が記載される。認証の認証情報は、モバイル装置からアクセスされるサービスがハンドオフ中にシームレスに中断せずに継続するように生成することができる。本明細書に記載されるように、アクセス層で第１のネットワークエンティティとの間にセキュアな通信を確立することができる。第１のネットワークエンティティとのセキュアな通信に基づいて、セキュアなアプリケーション層の通信をアプリケーションサーバとの間にも確立することができる。サービスはセキュアな通信を使用して受信することができる。第２のネットワークエンティティを発見することができる。第２のネットワークエンティティに対する認証のために認証の認証情報（例えば、アクセス層の認証情報）を生成することができる。認証の認証情報は、アプリケーション層の通信に関連付けられたアプリケーション層の情報を使用して生成することができる。認証の認証情報は、ハンドオフ中にサービスがシームレスに中断されずに生成されうる。

【００１４】
例示的実施形態によると、認証は、例えばシングルサインオン（ＳＳＯ）プロトコルを使用して１つのネットワークから別のネットワークへのハンドオフ時に行って、アプリケーションサーバからのサービスにワイヤレス通信装置がアクセスできるようにすることができる。例えば、ハンドオフは、セルラ通信ネットワーク（例えば、３ＧＰＰネットワーク）からワイヤレスローカルエリアネットワーク（ＷＬＡＮ）（例えば、ブラウザベースのＷＬＡＮまたは８０２．１ｘ／ＥＡＰに基づくＷＬＡＮ）へと行われることができる。ＳＳＯプロトコルは、汎用ブートストラッピングアーキテクチャ（ＧＢＡ）に基づくことができる。ＳＳＯプロトコルはＯｐｅｎＩＤを実装することもできる。ＳＳＯプロトコルを使用して、例えば逆ブートストラップなどの鍵導出機能を実装して、アプリケーションサーバでユーザおよび／または装置を認証するために使用される認証の認証情報を生成することができる。アプリケーションサーバは、ＯｐｅｎＩＤプロバイダ（ＯＰ）またはリライングパーティ（ＲＰ）として機能する、認証、認可および課金（ＡＡＡ）サーバを含むことができる。別の実施形態によると、アプリケーションサーバは、ＲＰとして機能するワイヤレスローカルエリアネットワーク（ＷＬＡＮ）ゲートウェイまたはＷＬＡＮアクセスポイント（ＡＰ）を含むことができる。ＷＬＡＮ　ＡＰは、ＵＥと別のＳＳＯエンティティとの間のＳＳＯの交換を可能にすることができる。

【００１５】
本明細書で使用される用語の説明を提供する。「ローカル識別プロバイダ（ローカルＩｄＰ）」は、ローカルに、すなわち装置上で、またはその非常に近くで行われるユーザ／装置の識別のアサーション（assertion）を可能にするクライアントのローカルにあるエンティティおよびそのようなエンティティの機能を意味する用語である。「ＲＰ」は、ＯｐｅｎＩＤプロトコルのリライングパーティまたは他のアプリケーションサービスプロバイダであり、ユーザ／装置の識別の検証を試み、識別プロバイダとの間に信頼関係を有する。「ＯＰ」は、ＯｐｅｎＩＤプロトコルのＯｐｅｎＩＤプロバイダまたはアプリケーションサービスプロバイダに代わってユーザおよび／または装置を認証することができる識別プロバイダである。「ＧＷ」は、例えば接続されたエンティティ間のインターネットトラフィックを制御するエンティティなどのゲートウェイである。「ＢＡ」は、ブラウジングエージェントである。「Ｕ」は一般的なモバイルユーザである。「ＵＥ」は一般的なモバイルユーザのモバイル装置である。

【００１６】
「ローカルモバイルＳＳＯ」は、従来はウェブベースのＳＳＯサーバによって行われていたシングルサインオン（ＳＳＯ）および／またはそれに関連する識別管理機能の一部またはすべてを装置上でローカルに行う方法を総称的に指すために使用される用語である。ローカルモバイルＳＳＯは、ローカルにあるエンティティおよび／またはモジュールによって行うことができ、それらのエンティティおよび／またはモジュールは例えば通信装置自体の一部または全体である。ローカルにあるエンティティ／モジュールは、通信装置および／またはそのユーザの近傍に物理的および／または論理的に位置する（すなわちローカルに位置する）ことができる（例えばそのようなエンティティ／モジュールが装置に内蔵されるか、ローカルインタフェースまたは配線または短距離のワイヤレス手段で装置に取り付けまたは接続される）。

【００１７】
「ローカルＯｐｅｎＩＤ」は、ＳＳＯまたは識別の管理をＯｐｅｎＩＤプロトコルに基づかせることができるローカルモバイルＳＳＯのサブセットの意味で使用される用語である。ＯｐｅｎＩＤ識別プロバイダ（ＯＰまたはＯｐｅｎＩＤ　ＩｄＰ）の機能の一部またはすべてを、ローカルに位置するエンティティ／モジュールによって行うことができる。

【００１８】
「ローカルＯＰ」は、ＯｐｅｎＩＤサーバの機能の一部またはすべてを行うエンティティまたはモジュールの意味で使用される用語である。ローカルＯＰは、ＯｐｅｎＩＤプロトコルを使用して実装されるローカルＩｄＰとすることができる。用語「ローカルＯＰ」

は、本明細書に記載される実施形態で実施することができるが、ローカルＩｄＰは、ＯｐｅｎＩＤプロトコルを実装しない同様の実施形態でも使用できることが理解されよう。「ＯＰｌｏｃ」をローカルのＯＰを意味するために使用する場合もある。ローカルＯＰの機能の１つは、ユーザおよび／または装置の識別についてのアサーションを通じてユーザおよび／またはワイヤレス通信装置の認証を容易にすることである。そのようなアサーションは、ローカルＯＰから装置（例えば、装置のブラウザエージェント）に送信することができ、装置はそのアサーションを外部のリライングパーティ（ＲＰ）に転送することができる。ローカルＯＰによって提供される機能が主にそのような識別のアサーションの提供に限られる場合は、そのような機能を行うローカルエンティティをローカルアサーションプロバイダ（ＬＡＰ）と呼ぶことができる。

【００１９】

ローカルＯＰは、１つまたは複数のアサーションメッセージを処理（例えば、作成、管理、および／または送信）することができる。ローカルＯＰは、そのメッセージを使用してユーザおよび／または装置に関連する１つまたは複数の識別の検証の状態をアサートすることができる。このアサーションは、そのようなメッセージの１つまたは複数の外部受信者に対して行うことができる。例えばリライングパーティ（ＲＰ）などの第３者エンティティがそのようなアサーションメッセージの受信者の１つとなることができる。ローカルＯＰは、例えば暗号鍵を使用する等してそのようなアサーションメッセージに署名することができる。

【００２０】

ローカルＯｐｅｎＩＤの方法では１つまたは複数の暗号鍵を使用することができる。そのような鍵の１つは、ルートセッション鍵と呼ばれるものであり、Ｋｒｐで表すことができ、これは、そこから他の鍵を導出できるルートセッション鍵の役割を果たすようにＲＰとＯＰとの間で使用されることが意図されるセッション鍵である。別のそのような鍵は、アサーション鍵と呼ばれるものであり、Ｋａｓｃと表すことができ、これは、ユーザの認証用のアサーションメッセージの１つまたは複数に署名するために使用できる署名鍵である。ＫａｓｃはＫｒｐから導出することができる。

【００２１】

ローカルＯｐｅｎＩＤは、ＯｐｅｎＩＤサーバ機能（ＯＰＳＦ）と呼ばれるサービスを使用して実装することもでき、その役割は、ローカルＯＰおよび任意でリライングパーティ（ＲＰ）に使用される秘密を生成、共有、および／または配布することである。ＯＰＳＦおよびローカルＯＰは、外部のＲＰからは１つのエンティティとして見える。ＯＰＳＦは、ローカルＯＰによって発行された署名を検証することができ、例えば公衆のインターネットまたは他の有線もしくは無線の通信を介してＲＰに直接到達することができる。装置は、例えばＯＰＳＦのアドレスがローカルＯＰに対応付けられるように装置上のローカルＤＮＳリゾルビングキャッシュ（resolving cache）を変更する等により、（例えばブラウザを介して）ローカルＯＰにリダイレクトされることができる。ローカルＯｐｅｎＩＤは、「ＯＰ－ａｇｇ」と表されるサービスを使用することもでき、その役割は、ＲＰに代わってローカルＯＰの発見を容易にすることである。

【００２２】

上述の用語および説明が本明細書に記載される実施形態で参照される場合がある。本明細書の実施形態はＯｐｅｎＩＤの用語および／またはＯｐｅｎＩＤプロトコルの一部を使用して説明することができるが、それらの実施形態は、ＯｐｅｎＩＤプロトコルまたはＯｐｅｎＩＤエンティティの使用に限定されないことが理解されよう。

【００２３】

例示的実施形態によると、本明細書にさらに説明するように、例えばスマートフォンなどのモバイル通信装置は、階層化された通信を使用して通信することができる。モバイル通信装置は、アクセス層で例えばアクセス層ネットワークとの間に通信を確立することができる。モバイル通信装置は、アプリケーション層またはアクセス層でも、アプリケーションサービスプロバイダおよび／またはそのようなプロバイダのそれぞれアプリケーショ

ン層ネットワークまたはアクセスネットワーク等との間に通信を確立することができる。各層で、通信はそれぞれ独自のセキュリティを有することができる。そのような層固有のセキュリティは、各層で認証および／またはセキュリティ鍵の合意を実装することができる。例えばアプリケーション層などの上位層における認証および／またはセキュリティ鍵の合意では、セキュリティ鍵および／または他のセキュリティ関連情報、例えば下位層のセキュリティの関連付けのコンテクストを利用して、アプリケーション層のための鍵または他のセキュリティ関連パラメータを導出することができる。そのような技術は、例えばブートストラッピング技術と呼ばれることがある。

【００２４】

例示的実施形態によると、モバイル装置がそのアクセス層通信をあるアクセスネットワークから別のアクセスネットワークに切り替える時、そのような工程をアクセス層のハンドオフと呼ぶことがある。アクセス層のハンドオフは、例えば通信を行っている装置の移動に起因して発生する。アクセス層のハンドオフは、アクセス層ネットワーク内の例えば基地局などの１つのアクセス層ノードと、例えば別の基地局などの別のそのようなノードとの間で発生する。２つのアクセス層ノードは、例えば、同じネットワーク内にある場合も、あるアクセス層ネットワークと別のアクセス層ネットワーク、すなわち異なるアクセス層ネットワークにある場合もある。アクセス層のハンドオフは、モバイル通信装置のユーザに対して透過であることが望ましい場合がある。また、アクセス層のハンドオフは、アプリケーション層の通信の継続した滑らかな動作を行うために中断がないことも望ましい場合がある。

【００２５】

アプリケーション層のセキュリティ認証情報を使用して、例えばアクセス層の状況時などにアクセス層のセキュリティの確立を助けることができる。例示的実施形態によると、例えばＯｐｅｎＩＤを実装することが可能な委託認証をアプリケーション層で行って、ハンドオフ時の後続ネットワークへのアクセス時に発見および／または接続を支援することができる。

【００２６】

一実施形態によると、ブートストラップを使用することができる。アクセス層のセキュリティ鍵を、既存のアプリケーション層の通信で入手できるセキュリティ材料から導出することができる。例えば、アクセス層のセキュリティ鍵は、例えばＧＢＡまたはＯｐｅｎＩＤなどの委託形態の認証を使用して確立されたセキュリティ材料から導出することができる。

【００２７】

別の実施形態によると、逆ブートストラップを使用することができる。アクセス層のセキュリティ鍵は、既存のアプリケーション層の通信で入手可能なセキュリティ材料から導出することができる。例えば、アクセス層のセキュリティ鍵は、例えばＯｐｅｎＩＤなどの委託形態の認証を使用して確立されたセキュリティ材料から導出することができる。

【００２８】

本明細書に記載されるように、認証を行う際にはローカルのアサーションプロバイダも使用することができる。例えば、ローカルＯＰを、アプリケーション層で使用されるＯｐｅｎＩＤプロトコルの一部として使用することができる。ローカルＯＰは、アクセス層のハンドオフ時にシームレスな認証および／または鍵合意を容易にすることができる。アクセス層の認証および／または鍵合意ならびにアクセス層の認可を、シームレスなハンドオフ中に可能にすることができる。

【００２９】

図１Ａ～１Ｃに、本明細書に記載される実施形態で実装することが可能なネットワーク通信システムおよび／または装置の例を示す。図１Ａは、１つまたは複数の開示実施形態を実施することが可能な例示的通信システム１００の図である。通信システム１００は、音声、データ、映像、メッセージング、放送等のコンテンツを複数のワイヤレスユーザに提供する多重接続システムとすることができる。通信システム１００は、複数のワイヤレ

スユーザが、ワイヤレス帯域幅を含むシステム資源の共有を通じてそのようなコンテンツにアクセスすることを可能にすることができる。例えば、通信システム１００は、符号分割多重接続（ＣＤＭＡ）、時分割多重接続（ＴＤＭＡ）、周波数分割多重接続（ＦＤＭＡ）、直交ＦＤＭＡ（ＯＦＤＭＡ）、単一キャリアＦＤＭＡ（ＳＣ－ＦＤＭＡ）等の１つまたは複数のチャネルアクセス方法を用いることができる。

【００３０】

図１Ａに示すように、通信システム１００は、ワイヤレス送信／受信ユニット（ＷＴＲＵ）１０２ａ、１０２ｂ、１０２ｃ、１０２ｄ、無線アクセスネットワーク（ＲＡＮ）１０４、コアネットワーク１０６、公衆交換電話網（ＰＳＴＮ）１０８、インターネット１１０、および他のネットワーク１１２を含むことができる。ただし、開示される実施形態では、任意の数のＷＴＲＵ、基地局、ネットワーク、および／またはネットワーク要素を企図することが理解されよう。各ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄは、ワイヤレス環境で動作および／または通信するように構成された任意の種類の装置であってよい。例として、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄは、ワイヤレス信号を送信および／または受信するように構成することができ、ユーザ機器（ＵＥ）、移動局、固定型または移動型の加入者ユニット、タブレット、ページャ、携帯電話、携帯情報端末（ＰＤＡ）、スマートフォン、ラップトップ機、ネットブック、パーソナルコンピュータ、ワイヤレスセンサ、消費者電子製品等を含むことができる。

【００３１】

通信システム１００は、基地局１１４ａおよび基地局１１４ｂも含むことができる。各基地局１１４ａ、１１４ｂは、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄの少なくとも１つとワイヤレスにインタフェースを取って、コアネットワーク１０６、インターネット１１０、および／またはネットワーク１１２等の１つまたは複数の通信ネットワークへのアクセスを容易にするように構成された任意の種類の装置であってよい。例として、基地局１１４ａ、１１４ｂは、ベーストランシーバ局（ＢＴＳ）、ノードＢ、ｅノードＢ、ホームノードＢ、ホームｅノードＢ、サイトコントローラ、アクセスポイント（ＡＰ）、ワイヤレスルータ等である。図では基地局１１４ａ、１１４ｂは１つの要素としてそれぞれ図示するが、基地局１１４ａ、１１４ｂは任意の数の相互接続された基地局および／またはネットワーク要素を含んでよいことは理解されよう。

【００３２】

基地局１１４ａは、ＲＡＮ１０４の一部とすることができ、ＲＡＮ１０４は、他の基地局および／または、基地局コントローラ（ＢＳＣ）、無線ネットワークコントローラ（ＲＮＣ）、中継ノード等のネットワーク要素（図示せず）も含むことができる。基地局１１４ａおよび／または基地局１１４ｂは、セルと呼ぶ場合もある特定の地理領域（図示せず）内でワイヤレス信号を送信および／または受信するように構成することができる。セルはさらにセルセクタに分割することができる。例えば、基地局１１４ａに関連付けられたセルを３つのセクタに分割することができる。そのため、一実施形態では、基地局１１４ａは、３つのトランシーバ、すなわちセルのセクタごとに１つのトランシーバを含むことができる。一実施形態では、基地局１１４ａは、多入力多出力（ＭＩＭＯ）技術を用いることができ、したがってセルの各セクタに複数のトランシーバを利用することができる。

【００３３】

基地局１１４ａ、１１４ｂは、エアインタフェース１１６を通じてＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄの１つまたは複数と通信することができる。エアインタフェース１１６は、任意の適切なワイヤレス通信リンク（例えば無線周波（ＲＦ）、マイクロ波、赤外線（ＩＲ）、紫外線（ＵＶ）、可視光等）であってよい。エアインタフェース１１６は、適切な無線アクセス技術（ＲＡＴ）を使用して確立することができる。

【００３４】

より具体的には、上記で述べたように、通信システム１００は多重接続システムであってよく、ＣＤＭＡ、ＴＤＭＡ、ＦＤＭＡ、ＯＦＤＭＡ、ＳＣ－ＦＤＭＡ等の１つまたは複数のチャネルアクセス方式を用いることができる。例えば、ＲＡＮ１０４の基地局１１４

ａとＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃは、Universal Mobile Telecommunication System（ＵＭＴＳ）Terrestrial Radio Access（ＵＴＲＡ）等の無線技術を実装することができ、その場合は広帯域ＣＤＭＡ（ＷＣＤＭＡ（登録商標））を使用してエアインタフェース１１６を確立することができる。ＷＣＤＭＡは、High－Speed Packet Access（ＨＳＰＡ）および／またはEvolved ＨＳＰＡ（ＨＳＰＡ＋）等の通信プロトコルを含むことができる。ＨＳＰＡはHigh－Speed Downlink Packet Access（ＨＳＤＰＡ）および／またはHigh－Speed Uplink Packet Access（ＨＳＵＰＡ）を含むことができる。

【００３５】

一実施形態では、基地局１１４ａおよびＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃは、Evolved ＵＭＴＳ Terrestrial Radio Access（Ｅ－ＵＴＲＡ）等の無線技術を実装することができ、その場合、エアインタフェース１１６はLong Term Evolution（ＬＴＥ）および／またはＬＴＥ－Advanced（ＬＴＥ－Ａ）を使用して確立することができる。

【００３６】

他の実施形態では、基地局１１４ａおよびＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃは、ＩＥＥＥ８０２．１６（すなわちWorldwide Interoperability for Microwave Access（ＷｉＭＡＸ））、ＣＤＭＡ２０００、ＣＤＭＡ２０００　１Ｘ、ＣＤＭＡ２０００　ＥＶ－ＤＯ、Interim Standard　２０００（ＩＳ－２０００）、Interim Standard　９５（ＩＳ－９５）、Interim Standard　８５６（ＩＳ－８５６）、Global System for Mobile Communication（ＧＳＭ（登録商標））、Enhanced Data rates for ＧＳＭ Evolution（ＥＤＧＥ）、ＧＳＭＥＤＧＥ（ＧＥＲＡＮ）等の無線技術を実装することができる。

【００３７】

図１Ａの基地局１１４ｂは、例えばワイヤレスルータ、ホームノードＢ、ホームｅノードＢ、フェムトセルの基地局、またはアクセスポイントであり、職場、家庭、乗り物、学校構内等の局所的な領域内でのワイヤレス接続を容易にする任意の適切なＲＡＴを利用することができる。一実施形態では、基地局１１４ｂおよびＷＴＲＵ１０２ｃ、１０２ｄは、ＩＥＥＥ８０２．１１等の無線技術を実装してワイヤレスローカルエリアネットワーク（ＷＬＡＮ）を確立することができる。一実施形態では、基地局１１４ｂおよびＷＴＲＵ１０２ｃ、１０２ｄは、ＩＥＥＥ８０２．１５等の無線技術を実装してワイヤレスパーソナルエリアネットワーク（ＷＰＡＮ）を確立することができる。さらに一実施形態では、基地局１１４ｂおよびＷＴＲＵ１０２ｃ、１０２ｄは、セルラ方式のＲＡＴ（例えばＷＣＤＭＡ、ＣＤＭＡ２０００、ＧＳＭ、ＬＴＥ、ＬＴＥ－Ａ等）を利用してピコセルまたはフェムトセルを確立することができる。図１Ａに示すように、基地局１１４ｂは、インターネット１１０への直接の接続を有することができる。そのため、基地局１１４ｂは、コアネットワーク１０６を介してインターネット１１０にアクセスする必要がない場合もある。

【００３８】

ＲＡＮ１０４はコアネットワーク１０６と通信状態にあることができ、コアネットワークは、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄの１つまたは複数に音声、データ、アプリケーション、および／またはVoice over Internet Protocol（ＶｏＩＰ）サービスを提供するように構成された任意の種類のネットワークであってよい。例えば、コアネットワーク１０６は、呼制御、課金サービス、モバイル位置を利用するサービス、料金前払いの通話、インターネット接続、映像配布等を提供する、および／またはユーザ認証等の高レベルのセキュリティ機能を行うことができる。図１Ａには示さないが、ＲＡＮ１０４および／またはコアネットワーク１０６は、ＲＡＮ１０４と同じＲＡＴまたは異なるＲＡＴを用いる他のＲＡＮと直接通信状態にあっても、または間接的な通信状態にあってもよいことが理解されよう。例えば、Ｅ－ＵＴＲＡ無線技術を利用する可能性のあるＲＡＮ１０４に接続されるのに加えて、コアネットワーク１０６は、ＧＳＭ無線技術を用いる別のＲＡＮ（図示せず）とも通信状態にあることができる。

【００３９】

コアネットワーク１０６は、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄがＰＳ

ＴＮ１０８、インターネット１１０および／または他のネットワーク１１２にアクセスするためのゲートウェイの役割を果たすこともできる。ＰＳＴＮ１０８は、従来の電話サービス（ＰＯＴＳ）を提供する回線交換電話網を含むことができる。インターネット１１０は、ＴＣＰ／ＩＰインターネットプロトコルスイートの伝送制御プロトコル（ＴＣＰ）、ユーザデータグラムプロトコル（ＵＤＰ）、インターネットプロトコル（ＩＰ）等の一般的な通信プロトコルを使用する相互接続されたコンピュータネットワークおよび装置からなる世界規模のシステムを含むことができる。ネットワーク１１２は、他のサービス提供者に所有および／または運営される有線またはワイヤレスの通信ネットワークを含むことができる。例えば、ネットワーク１１２は、ＲＡＮ１０４と同じＲＡＴまたは異なるＲＡＴを用いる可能性のある１つまたは複数のＲＡＮに接続された別のコアネットワークを含むことができる。

【００４０】

通信システム１００内のＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄの一部またはすべては、多モード機能を備えることができる。すなわち、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄは、種々のワイヤレスリンクを通じて種々のワイヤレスネットワークと通信するための複数のトランシーバを含むことができる。例えば、図１Ａに示すＷＴＲＵ１０２ｃは、セルラ方式の無線技術を用いる可能性のある基地局１１４ａ、およびＩＥＥＥ８０２無線技術を用いる可能性のある基地局１１４ｂと通信するように構成することができる。

【００４１】

図１Ｂは、例示的なＷＴＲＵ１０２のシステム図である。図１Ｂに示すように、ＷＴＲＵ１０２は、プロセッサ１１８、トランシーバ１２０、送信／受信要素１２２、スピーカ／マイクロフォン１２４、キーパッド１２６、ディスプレイ／タッチパッド１２８、取外し不能メモリ１３０、取外し可能メモリ１３２、電源１３４、全地球測位システム（ＧＰＳ）チップセット１３６、および他の周辺機能１３８を備えることができる。ＷＴＲＵ１０２は、実施形態との整合性を保ちながら、上述の要素の任意のサブコンビネーションを含むことが可能であることが理解されよう。

【００４２】

プロセッサ１１８は、汎用プロセッサ、特殊目的プロセッサ、従来のプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、複数のマイクロプロセッサ、ＤＳＰコアと関連した１つまたは複数のマイクロプロセッサ、コントローラ、マイクロコントローラ、特定用途集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）回路、任意の他の種類の集積回路（ＩＣ）、状態機械等である。プロセッサ１１８は、信号の符号化、データ処理、電力制御、入出力処理、および／またはＷＴＲＵ１０２がワイヤレス環境で動作することを可能にする任意の他の機能を行うことができる。プロセッサ１１８はトランシーバ１２０に結合することができ、トランシーバ１２０は送信／受信要素１２２に結合することができる。図１Ｂではプロセッサ１１８とトランシーバ１２０を別個の構成要素として示すが、プロセッサ１１８とトランシーバ１２０は電子パッケージやチップに共に一体化してよいことが理解されよう。プロセッサ１１８は、アプリケーション層のプログラム（例えば、ブラウザ）および／または無線アクセス層（ＲＡＮ）のプログラムおよび／または通信を行うことができる。プロセッサ１１８は、例えばアクセス層および／またはアプリケーション層における、認証、セキュリティ鍵の合意、および／または暗号動作などのセキュリティ動作を行うことができる。

【００４３】

送信／受信要素１２２は、エアインタフェース１１６を通じて基地局（例えば基地局１１４ａ）との間で信号を送信または受信するように構成することができる。例えば、一実施形態では、送信／受信要素１２２は、ＲＦ信号を送信および／または受信するように構成されたアンテナとすることができる。一実施形態では、送信／受信要素１２２は、例えばＩＲ、ＵＶ、または可視光信号を送信および／または受信するように構成されたエミッタ／検出器とすることができる。一実施形態では、送信／受信要素１２２は、ＲＦ信号と

光信号の両方を送受信するように構成することができる。送信／受信要素１２２は、各種ワイヤレス信号の任意の組合せを送信および／または受信するように構成してよいことが理解されよう。

【００４４】

また、図１Ｂでは送信／受信要素１２２を１つの要素として示すが、ＷＴＲＵ１０２は任意の数の送信／受信要素１２２を含んでよい。より具体的には、ＷＴＲＵ１０２はＭＩＭＯ技術を用いることができる。そのため、一実施形態では、ＷＴＲＵ１０２は、エアインタフェース１１６を通じてワイヤレス信号を送受信するために２つ以上の送信／受信要素１２２（例えば複数のアンテナ）を含むことができる。

【００４５】

トランシーバ１２０は、送信／受信要素１２２によって送信される信号を変調し、送信／受信要素１２２によって受信された信号を復調するように構成することができる。上記のように、ＷＴＲＵ１０２は多モード機能を有することができる。そのため、トランシーバ１２０は、ＷＴＲＵ１０２が例えばＵＴＲＡやＩＥＥＥ８０２．１１等の複数のＲＡＴを介して通信することを可能にする複数のトランシーバを含むことができる。

【００４６】

ＷＴＲＵ１０２のプロセッサ１１８は、スピーカ／マイクロフォン１２４、キーパッド１２６、および／またはディスプレイ／タッチパッド１２８（例えば液晶ディスプレイ（ＬＣＤ）表示装置または有機発光ダイオード（ＯＬＥＤ）表示装置）に結合し、それらからユーザ入力データを受け取ることができる。プロセッサ１１８は、スピーカ／マイクロフォン１２４、キーパッド１２６、および／またはディスプレイ／タッチパッド１２８にユーザデータを出力することもできる。また、プロセッサ１１８は、取外し不能メモリ１３０および／または取外し可能メモリ１３２等の任意の種類の適切なメモリからの情報にアクセスし、これらにデータを記憶することができる。取外し不能メモリ１３０は、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、ハードディスク、および／または任意の他の種類のメモリ記憶装置を含むことができる。取外し可能メモリ１３２は、加入者識別モジュール（ＳＩＭ）カード、メモリスティック、セキュアデジタル（ＳＤ）メモリカード等を含むことができる。他の実施形態では、プロセッサ１１８は、サーバや家庭コンピュータ（図示せず）等、物理的にＷＴＲＵ１０２に位置しないメモリからの情報にアクセスし、そのメモリにデータを記憶することができる。

【００４７】

プロセッサ１１８は、電源１３４から電力を受け取り、その電力をＷＴＲＵ１０２中の他の構成要素に分配および／または制御するように構成することができる。電源１３４は、ＷＴＲＵ１０２に電力を供給するのに適した任意の装置でよい。例えば、電源１３４は、１つまたは複数の乾電池（例えばニッケルカドミウム（ＮｉＣｄ）、ニッケル亜鉛（ＮｉＺｎ）、ニッケル水素（ＮｉＭＨ）、リチウムイオン（Ｌｉ－ｉｏｎ）等）、太陽電池、燃料電池等を含むことができる。

【００４８】

プロセッサ１１８はＧＰＳチップセット１３６にも結合することができ、ＧＰＳチップセット１３６は、ＷＴＲＵ１０２の現在の位置に関する位置情報（例えば経度および緯度）を提供するように構成することができる。ＧＰＳチップセット１３６からの情報に加えて、またはその代わりに、ＷＴＲＵ１０２は、基地局（例えば基地局１１４ａ、１１４ｂ）からエアインタフェース１１６を介して位置情報を受信し、および／または、２つ以上の近隣の基地局から信号が受信されるタイミングに基づいて自身の位置を判定することもできる。ＷＴＲＵ１０２は、実施形態との整合性を保ちながら、任意の適切な位置判定方法で位置情報を取得してよいことが理解されよう。

【００４９】

プロセッサ１１８はさらに他の周辺機能１３８に結合することができ、それらは、追加的な機能、機能性、および／または有線もしくは無線接続を提供する１つまたは複数のソフトウェアおよび／またはハードウェアモジュールを含むことができる。例えば、周辺機

能１３８は、加速度計、電子コンパス、衛星トランシーバ、デジタルカメラ（写真または映像用）、ユニバーサルシリアルバス（ＵＳＢ）ポート、振動装置、テレビトランシーバ、ハンドフリーヘッドセット、Ｂｌｕｅｔｏｏｔｈ（登録商標）モジュール、周波数変調（ＦＭ）無線ユニット、デジタル音楽プレーヤ、メディアプレーヤ、ビデオゲームプレーヤモジュール、インターネットブラウザ等を含むことができる。

【００５０】

図１Ｃは、一実施形態によるＲＡＮ１０４およびコアネットワーク１０６のシステム図である。上記のように、ＲＡＮ１０４は、ＵＴＲＡ無線技術を用いてエアインタフェース１１６を介してＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃと通信することができる。ＲＡＮ１０４は、コアネットワーク１０６とも通信状態にあることができる。図１Ｃに示すように、ＲＡＮ１０４は、ノードＢ１４０ａ、１４０ｂ、１４０ｃを含み、ノードＢ１４０ａ、１４０ｂ、１４０ｃは各々、エアインタフェース１１６を通じてＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃと通信するために１つまたは複数のトランシーバを含むことができる。ノードＢ１４０ａ、１４０ｂ、１４０ｃは各々、ＲＡＮ１０４内の特定のセル（図示せず）に関連付けることができる。ＲＡＮ１０４はＲＮＣ１４２ａ、１４２ｂも含むことができる。ＲＡＮ１０４は実施形態との整合性を保ちながら、任意の数のノードＢおよびＲＮＣを含むことが可能であることが理解されよう。

【００５１】

図１Ｃに示すように、ノードＢ１４０ａ、１４０ｂはＲＮＣ１４２ａと通信状態にあることができる。また、ノードＢ１４０ｃはＲＮＣ１４２ｂと通信状態にあることができる。ノードＢ１４０ａ、１４０ｂ、１４０ｃは、Ｉｕｂインタフェースを介してそれぞれのＲＮＣ１４２ａ、１４２ｂと通信することができる。ＲＮＣ１４２ａ、１４２ｂは、Ｉｕｒインタフェースを介して互いに通信することができる。各ＲＮＣ１４２ａ、１４２ｂは、それぞれが接続されたノードＢ１４０ａ、１４０ｂ、１４０ｃを制御するように構成することができる。また、各ＲＮＣ１４２ａ、１４２ｂは、外部ループ電力制御、負荷制御、アドミッション制御、パケットのスケジューリング、ハンドオーバー制御、マクロダイバーシティ、セキュリティ機能、データ暗号化等の他の機能を実行および／または支援するように構成することができる。

【００５２】

図１Ｃに示すコアネットワーク１０６は、メディアゲートウェイ（ＭＧＷ）１４４、モバイル交換センター（ＭＳＣ）１４６、サービングＧＰＲＳサポートノード（ＳＧＳＮ）１４８、および／またはゲートウェイＧＰＲＳサポートノード（ＧＧＳＮ）１５０を含むことができる。上記の各要素はコアネットワーク１０６の一部として図示するが、これらの要素の任意の１つはコアネットワークの運営者以外のエンティティにより所有および／または運営され得ることが理解されよう。

【００５３】

ＲＡＮ１０４内のＲＮＣ１４２ａは、ＩｕＣＳインタフェースを介してコアネットワーク１０６内のＭＳＣ１４６に接続することができる。ＭＳＣ１４６はＭＧＷ１４４に接続することができる。ＭＳＣ１４６およびＭＧＷ１４４は、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃに、ＰＳＴＮ１０８等の回線交換ネットワークへのアクセスを提供して、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃと従来の固定電話機器との間の通信を容易にすることができる。

【００５４】

ＲＡＮ１０４内のＲＮＣ１４２ａは、ＩｕＰＳインタフェースを介してコアネットワーク１０６のＳＧＳＮ１４８にも接続することができる。ＳＧＳＮ１４８はＧＧＳＮ１５０に接続することができる。ＳＧＳＮ１４８およびＧＧＳＮ１５０は、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃに、インターネット１１０等のパケット交換ネットワークへのアクセスを提供して、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃとＩＰ対応機器との間の通信を容易にすることができる。

【００５５】

上記のように、コアネットワーク１０６はネットワーク１１２にも接続することができ、ネットワーク１１２は、他のサービス提供者によって所有および／または運営される有線または無線のネットワークを含む。

【００５６】

上記の通信システムおよび／または装置を、本明細書に記載される認証ハンドオフのシナリオで使用することができる。認証ハンドオフは、ユーザが、アクセスネットワーク間、および／または同じもしくは異なるアクセスネットワーク内のアクセスポイント間を切り替わる間にサービスおよび／またはアプリケーションを継続的に使用できるようにすることができる。ハンドオフの決定は、例えばアクセス層および／またはアプリケーション層で行うことができる。これは、各層における認証がハンドオフのたびに行われること、および／またはユーザ装置に移動先のネットワーク／アクセスポイントのための認証情報を事前に供給しておく場合があることを意味する。それには、集中化された基盤および／または認証情報の事前供給が必要となる可能性がある。独立した委託認証エンティティを使用すると、複数形態のネットワーク間を移動する際のシームレスな認証を容易にする際のモバイルネットワーク事業者（ＭＮＯ）との複数のサービスレベル契約（ＳＬＡ）の確立や、ＭＮＯ認証用の基盤との緊密な結合を回避することができる。例えばＯｐｅｎＩＤなどの連携識別管理方式および／またはインターネットへのアクセスを、本明細書に記載される認証の実施形態で支援することができる。

【００５７】

事前に供給された認証情報を使用してアクセス層のハンドオフを行う装置の一例を図２に示し、この場合、装置２１５は２つのアクセスネットワーク間を切り替える。図２は、アプリケーション層のセッションの場合のハンドオフシナリオを説明する流れ図である。図２に示すハンドオフシナリオは装置２１５を含み、装置２１５は、アプリケーション層での通信が可能なアプリケーション２１４およびアクセス層での通信が可能なアクセス層モジュール２１６を含むか、またはそれらと通信状態にある。図２に示すハンドオフシナリオは、ＭＮＯ　Ａ　２１７、ホットスポットＢ　２１８、およびアプリケーションサーバ２１９も含むことができる。ＭＮＯ　Ａ　２１７および／またはホットスポットＢ　２１８は、各自のアプリケーション層機能で委託認証サーバの能力があるＯｐｅｎＩＤサーバ機能で使用可能とすることができる。委託形態の認証方法は例えばＯｐｅｎＩＤである。したがって、ＭＮＯ　Ａ　２１７を「ＭＮＯ　ＯｐｅｎＩＤプロバイダ（ＯＰ）Ａ　２１７」（すなわち、このエンティティがＭＮＯ　Ａのアクセス層の機能とＯｐｅｎＩＤのサーバ機能を有することができる）、および／またはホットスポットＢ　２１８を「ホットスポットＯＰ　Ｂ　２１８」と表すことができる。装置２１５は、アクセス層モジュール２１６を介してＭＮＯ　Ａ　２１７および／またはホットスポットＢ　２１８と通信することができる。装置２１５は、アプリケーション２１４を介してアプリケーションサーバ２１９とも通信することができる。

【００５８】

図２に示すように、装置２１５は、例えばモバイルネットワーク事業者（ＭＮＯ）Ａ　２１７のセルラネットワークと、例えばホットスポットＢ　２１８などのフェムトネットワークまたはＷＬＡＮネットワークとの間を切り替えることができる。装置２１５は、装置のアプリケーションおよび／またはネットワークアプリケーションサーバ２１９でブートストラップされたアクセス層の認証情報２２０を使用して、アプリケーション層の認証のためのアプリケーション層の認証情報２２１を作成することができる。そして、装置２１５は、ホットスポットＢ　２１８で後続ネットワーク（例えば、ＷＬＡＮネットワーク）にアタッチ（ａｔｔａｃｈ）し、装置２１５とホットスポットＢ　２１８との間で事前に供給された認証情報２２２を使用して認証を行うことができる。

【００５９】

図２に示すハンドオフシナリオに示すように、２０１で、装置２１５は、ＭＮＯ　Ａ　２１７のアクセスネットワークを発見することができる。装置２１５は、それぞれ２０２および２０３でＭＮＯ　Ａ　２１７のアクセスネットワークにアタッチおよび／または認

証することができる。例えば、装置２１５は、アクセス層モジュール２１６を介してＭＮＯ　Ａ　２１７のアクセスネットワークに対してアタッチおよび／または認証することができる。装置２１５は、認証の認証情報２２０を使用してＭＮＯ　Ａ　２１７に対して認証することができる。認証の認証情報２２０は、例えば装置２１５とＭＮＯ　Ａ　２１７間の事前に供給された認証情報とすることができる。２０３の認証が成功すると、装置２１５およびＭＮＯ　Ａ　２１７のアクセスネットワークは、２０４でアクセス層モジュール２１６を介してセキュアなアクセス層の通信を確立することができる。

【００６０】

装置２１５は、ＭＮＯ　Ａ　２１７のネットワークを使用してアプリケーションサーバ２１９へのログインを試みて、アプリケーションサーバ２１９からのサービスにアクセスすることができる。例えば、装置２１５のアプリケーション２１４が、２０５でネットワークベースのアプリケーションサーバ２１９にログインすることができる。アプリケーションサーバ２１９は、リライングパーティ（ＲＰ）として機能し、ＭＮＯ　Ａ　２１７はＯｐｅｎＩＤ識別プロバイダ（ＯＰ）として機能することができる。例えば、２０６で、アプリケーションサーバ２１９は、ＭＮＯ　Ａ　２１７を発見すること、および／またはＭＮＯ　Ａ　２１７にユーザを認証するように要求することができる。この要求および／または認証は、例えばＯｐｅｎＩＤを使用して行うことができる。２０７で、装置のアプリケーション２１４とＯＰとして機能するＭＮＯ　Ａ　２１７との間で、アプリケーション層の認証の認証情報２２１を、ＭＮＯ　Ａ　２１７のアクセス層に対する装置のアクセス層モジュール２１６のアクセス層認証を可能にしたアクセス層の認証情報２２０からブートストラップ（例えば生成または導出）することができる。装置２１５および／またはそのアプリケーション２１４は、２０８でＭＮＯ　Ａ　２１７にリダイレクトされ、アクセス層の認証情報２２０からブートストラップされたアプリケーション層の認証の認証情報２２１を使用してアプリケーション層でＭＮＯ　Ａ　２１７に対して認証することができる。２０７における認証情報２２１のブートストラップは、２０８の認証の一部として行っても、別個に行ってもよい。ＭＮＯ　Ａ　２１７は、装置２１５の認証ステータスをリライングパーティ（ＲＰ）（図示せず）として機能するアプリケーションサーバ２１９に対してアサートすることができる。２０９で、アプリケーション層のセキュアな通信を、装置のアプリケーション２１４とネットワークベースのアプリケーションサーバ２１９との間に確立することができる。

【００６１】

２１０で、装置のアクセス層モジュール２１６がホットスポットＢ　２１８を発見することができる。ホットスポットＢ　２１８は、ＷＬＡＮ上のノードとすることができ、装置２１５がアプリケーションサーバ２１９のサービスにアクセスすることを可能にする。例示的実施形態によると、装置２１５は、ホットスポットＢ　２１８のサービスエリアの範囲に入るとホットスポットＢ　２１８を発見することができる。装置２１５は、ユーザ設定、アプリケーション要件、ホットスポットの条件、および／または装置２１５に記憶されたサービスプロバイダのポリシに基づいてホットスポットＢ　２１８にアタッチを試みることができる。２１１で、装置２１５は、アクセス層モジュール２１６を介してアクセス層でホットスポットＢ　２１８にアタッチすることができる。一実施形態によると、２０９で確立されるアプリケーション層の接続は、２１１で行われる後続のアクセス層の（ホットスポットＢ　２１８への）アタッチ後も存続することができる。

【００６２】

２１２で、装置２１５は、認証情報２２２を使用してアクセス層モジュール２１６を介してホットスポットＢ　２１８に対して認証することができる。２１２で使用される認証情報２２２は、それぞれ２０３および２０８で認証に使用される認証情報２２０または認証情報２２１とは関係がなくてよい。したがって、２１２で、装置２１５に対する認証では、後続の移動先アクセスネットワーク（例えばホットスポットＢ　２１８）に適する可能性のある事前に供給されたアクセス層の認証情報２２２を使用することができる。２１２で認証が成功すると、２１３で装置２１５およびホットスポットＢ　２１８はアクセス

層でセキュアな通信を確立することができる。

【００６３】

上記のように、図２には、装置２１５が事前に供給された認証情報２２２を使用してハンドオフおよび／または後続ネットワークでアクセス層の認証を行えるようにする認証プロトコルを示す。本明細書には、ハンドオフ用のアクセス層またはアプリケーション層の認証情報などの持続的な認証情報を活用して、要求時にかつシームレスな方式で他の層（例えばアクセス層）における認証および／またはセキュアなトンネルの確立を完了するための各種実装も記載される。

【００６４】

例示的実施形態によると、アプリケーション層の認証情報を活用して、続く後続のアクセス層の認証手順で使用可能なアクセス層の認証情報を（例えばアプリケーション層の認証情報の逆ブートストラップを行うことにより）生成することができる。図３に示すように、ハンドオフシナリオでは、アプリケーション層の認証情報３３１の逆ブートストラップを実施して、後続ネットワークで認証を行うことができる。図３に示すハンドオフシナリオは装置３２１を含み、装置３２１は、アプリケーション層で通信可能なアプリケーション３２０およびアクセス層で通信可能なアクセス層モジュール３２２を含むか、それらと通信状態にある。アクセス層モジュール３２２は、装置３２１上の接続マネジャ（ＣＭ）を含む、および／または通信状態にあることができる。図３に示すハンドオフシナリオは、ＭＮＯ　Ａ　３２３、ホットスポットＢ　３２４、およびアプリケーションサーバ３２５も含む。ＭＮＯ　Ａ　３２３は、アクセス層３２６および／またはアプリケーション層３２７を介して他のネットワークエンティティと通信することができる。ＭＮＯ　Ａ　３２３はＯｐｅｎＩＤプロバイダとして機能することができる。ホットスポットＢ３２４は、アクセス層３２８および／またはアプリケーション層３２９を介して他のネットワークエンティティと通信することができる。ホットスポットＢ　３２４はリライングパーティ（ＲＰ）として機能することができる。アクセス層モジュール３２２は、ＭＮＯ　Ａ　３２３のアクセス層３２６および／またはホットスポットＢ　３２４のアクセス層３２８と通信することができる。アプリケーション３２０は、アプリケーションサーバ３２５、ＭＮＯ　Ａ　３２３のアプリケーション層３２７、および／またはホットスポットＢ　３２４のアプリケーション層３２９と通信することができる。アプリケーションサーバ３２５は、本明細書に記載のいくつかの実施形態によると、リライングパーティ（ＲＰ）として機能することもできる。

【００６５】

図３に示すように、例えばハンドオフのシナリオなどで、アプリケーション層の認証情報を生成し、逆ブートストラップして、後続アクセスネットワークのホットスポットＢ　３２４への認証のためのアクセス層の認証の認証情報３３３を生成することができる。逆ブートストラップは、移動先のアクセス層ネットワークのホットスポットＢ　３２４の代わりにＭＮＯ　Ａ　３２３によるアプリケーション層の認証を含み、後続のアクセス層の認証の認証情報３３３の生成に使用される材料を生成することができる。逆ブートストラップは、１）移動元ネットワークＭＮＯ　Ａ　３２３内のユーザ／装置３２１の識別、および／または、２）例えばアプリケーションサーバ３２５またはＭＮＯ　Ａ　３２３に関するユーザ／アプリケーション３２０のアプリケーション層の識別（例えばＯｐｅｎＩＤ識別）、の少なくとも１つを条件とすることができる。

【００６６】

ＭＮＯ　Ａ　３２３による以前の成功したアプリケーション層の認証を使用して、ネットワークホットスポットＢ　３２４へのアクセスを許可することができる。追加的な認証の情報をネットワークホットスポットＢ　３２４に提供して、装置３２１のアクセス層の認証を支援することができる。例えば、アサーション（例えば「ユーザはネットワークＭＮＯ　Ａ　３２３から移動して来て、認証済み」）がネットワークホットスポットＢ　３２４に提供されると、アプリケーション層の認証を使用してネットワークホットスポットＢ　３２４へのアクセスを許可することができる。

【００６７】
一実施形態によると、図３に示すように呼び出しのフローを提供することができる。３０１～３０９で、呼び出しのフローは、アプリケーション層のブートストラップ手順を使用してアクセス層のセキュリティの関連付けおよびアプリケーション層のセキュリティの関連付けを設定することができ、ブートストラップ手順でアクセス層の認証情報をＯｐｅｎＩＤの処理に結び付けることができる。例えば、３０１～３０４でアクセス層のセキュリティの関連付けを装置３２１とＭＮＯ　Ａ　３２３との間に確立することができる。３０１で、アクセス層モジュール３２２が、アクセス層３２６を介してＭＮＯ　Ａ　３２３のネットワークを発見することができる。アクセス層モジュール３２２は、３０２でＭＮＯ　Ａ　３２３にアタッチし、３０３で認証を行うことができる。３０３のアクセス層の認証は、装置３２１とＭＮＯ　Ａ　３２３との間で共有されるアクセス層の認証情報３３０を使用して行うことができる。アクセス層の認証情報３３０は、本明細書に記載されるように、事前に供給された認証情報であっても、または別のネットワークからのアプリケーション層の認証情報を逆ブートストラップすることによって確立された認証情報であってもよい。装置３２１とＭＮＯ　Ａ　３２３との間のアクセス層の認証が成功すると、３０４で装置３２１とＭＮＯ　Ａ　３２３との間にアクセス層３２６のセキュアな通信を確立することができる。

【００６８】
３０５～３０９でアプリケーション層のセキュリティの関連付けを装置３２１とアプリケーションサーバ３２５との間に確立することができる。例えば、３０５で、アプリケーション３２０がアプリケーションサーバ３２５へのログインを試みることができる。３０６で、アプリケーション層３２７を介してＭＮＯ　Ａ　３２３のＯＰサーバがアプリケーションサーバ３２５によって発見され、アプリケーションサーバ３２５はユーザ／装置３２１を認証のためにＭＮＯ　Ａ　３２３にリダイレクトすることができる。ＭＮＯ　Ａ　３２３のＯＰは、３０６でユーザ／装置３２１を認証するか、および／またはアプリケーションサーバ３２５に対してユーザ／装置３２１の認証をアサートすることができる。次いで、ユーザ／装置３２１をホットスポットＢ　３２４にリダイレクトすることができる。

【００６９】
３０７で、アプリケーション３２０とＭＮＯ　Ａ　３２３との間で、装置３２１とＭＮＯ　Ａ　３２３との間のアクセス層の認証を可能にしたアクセス層の認証情報３３０および／またはＭＮＯ　Ａ　３２３からの認証のアサーションからアプリケーション層の認証情報３３１をブートストラップ（例えば生成または導出）することができる。アプリケーション３２０およびアプリケーションサーバ３２５は、３０８で、アプリケーション層の認証情報３３１を使用してアプリケーション層のセキュリティの関連付けを設定することができる。３０８のアプリケーション層のセキュリティの関連付けの結果、アプリケーション層の認証情報がアプリケーション３２０とアプリケーションサーバ３２５との間で共有される。３０７の認証情報３３１のブートストラップは、３０８のアプリケーション層のセキュリティの関連付けの一部として行っても、独立して行ってもよい。３０９で、装置のアプリケーション３２０とネットワークベースのアプリケーションサーバ３２５との間にアプリケーション層のセキュアな通信を確立することができる。

【００７０】
３１０で、装置３２１がホットスポットＢ　３２４を発見することができる。例えば、装置３２１のローカルコンポーネント、例えばアクセス層モジュール３２２がホットスポットＢ　３２４および／またはその識別情報（例えば、ＳＳＩＤまたはＩＰアドレス）を発見することができる。ホットスポットＢのアプリケーション層３２９は発見可能にすることができ、そのＩＰアドレスなどのアクセス層３２８のネットワーク発見情報を使用して、例えば公衆のインターネットを介して発見および／または到達されている可能性がある。アクセス層モジュール３２２は接続マネジャ（ＣＭ）を含むことができ、接続マネジャは、ホットスポットＢ　３２４を発見し、および／または接続の決定を行う際に実装す

ることができる。ホットスポットＢ　３２４および／またはその識別情報は、例えばビーコンチャネルなどのアクセス層のシグナリングを介して発見することができる。ＭＮＯ　Ａ　３２３、ホットスポットＢ　３２４、および装置３２１から得られるホットスポットＢ　３２４についての発見された情報間の関係に基づいて、何らかの発見を行うことができる。ホットスポットＢ　３２４からの発見された情報（例えば信号の強度、位置等）に基づいて、装置３２１のアクセス層モジュール３２２は、装置３２１がネットワーク通信のためにホットスポットＢ　３２４に切り替わるべきであると判断することができる。アクセス層モジュール３２２はその指令を装置のアプリケーション３２０に伝えることができる。例えば、３１１でＣＭがアプリケーション層のネットワーク発見情報を装置のアプリケーション３２０に送信することができる。

【００７１】

装置３２１は、アプリケーション層とアクセス層との間でブートストラップ認証情報（例えば鍵導出処理を使用して生成された）の転送が可能となるように構成することができる。アプリケーション３２０は、ネットワーク発見情報を処理してアクセス層ネットワークに適した識別を生成することができる。一実施形態によると、ネットワークのアクセス層に適した識別は、ユーザ／装置３２１のＯｐｅｎＩＤ　ＵＲＬまたは電子メールアドレスログインであり、それをさらに処理／操作（例えばハッシュ処理して一意のユーザ／装置識別を生成する）して、アクセス層３２８のホットスポットＢ　３２４に対する識別に適した形式にすることができる。任意で、ノンス（nonce）またはシーケンスカウンタ値などの情報要素をハッシュ処理に加えるか、および／またはそれらの情報要素の一部をホットスポットＢ　３２４に通信してもよい。装置のアプリケーション３２０は、３０８で確立された自身のアプリケーション層識別および／またはホットスポットＢ　３２４のアクセス層発見情報に基づいて適切なアクセス層識別を決定することができる。アクセス層識別はアプリケーション層識別に結び付けられ、３１２で以後の送信のためにアクセス層モジュール３２２に送信されることができる。

【００７２】

３１３で、装置３２１は、アクセス層の適切な識別を使用してホットスポットＢ　３２４のアクセス層３２８にアタッチすることができ、装置のアクセス層モジュール３２２は、そのネットワークのアクセス層に適したアクセス層識別をホットスポットＢのアクセス層３２８に中継することができる。次いで、３１４で装置３２１のアクセス層識別をホットスポットＢのアプリケーション層３２９に渡し、装置のアクセス層識別子で装置３２１を識別できるようにアプリケーション層３２９に通知することができる。ホットスポットＢ　３２４のアプリケーション層３２９は、アクセス層３２８とは物理的に分離されるが、論理的に関連付けることができる。３１５で、装置３２１のアプリケーション３２０が、アプリケーション層の識別情報、および任意でアクセス層の識別をホットスポットＢのアプリケーション層３２９に送信することができる。このアプリケーション層の識別を提供して、例えばホットスポットＢ　３２４にログオンすることができる。アプリケーション層の識別は装置３２１のアクセス層識別に結び付けることができる。

【００７３】

アプリケーション層の識別およびアクセス層の識別情報がアプリケーション層３２９を介して通信されると、３１６でアプリケーション層の識別および／または発見されたホットスポットＢ　３２４の情報を使用して、ＯｐｅｎＩＤに基づくＭＮＯ　Ａ　３２３の発見を行うことができる。３１５の識別情報の送信は、例えば３１３から３１４の呼び出しフローと同時に行っても、または別の時に行ってもよい。アプリケーション層の識別情報の例は、例えば、ＯｐｅｎＩＤ　ＵＲＬまたは電子メールアドレスのログイン識別またはアサーションを含むことができる。識別情報は、ユーザ／装置３２１の補足情報も含むことができる。

【００７４】

ホットスポットＢ　３２４は、自身のアクセス層３２８から受け取るアクセス層の識別情報と、アプリケーション層３２９から受け取る結び付けられたアプリケーション層の識

別およびアクセス層の識別情報との両方を（例えばアクセス層で）統合および／または相関付けることができる。ホットスポットＢ　３２４は、３１３および３１５で受信したメッセージが同じユーザ／装置３２１からのものであるかどうかを判定することができる。例えば、アプリケーション層３２９で、ホットスポットＢ　３２４は、３１５で受け取ったアプリケーション層識別が３１４で受け取ったアクセス層識別に結び付けられていることを特定することができる。自身のアクセス層３２８およびアプリケーション層３２９で同じユーザ／装置３２１と通信していることを確認すると、ホットスポットＢ　３２４は、ＯＰとして機能するＭＮＯ　Ａ　３２３と共にＲＰとして機能することができる。ホットスポットＢ　３２４は、３１６でＭＮＯ　Ａ　３２３の発見を行い、認証のためにＭＮＯ　Ａ　３２３をユーザ／装置３２１に誘導することができる（例えばＯｐｅｎＩＤプロトコルの実行により）。装置のアプリケーション３２０は、ＭＮＯ　Ａのアプリケーション３２７に対して（例えばアプリケーション層３２７のＯＰで）認証することができる。認証が成功した後、装置３２１をリダイレクトしてホットスポットＢ　３２４のアプリケーション３２９に戻すことができる。３１７で、ホットスポットＢ　３２４および装置３２１は各々、鍵導出機能を使用して成功したアプリケーション層の認証からアクセス層の認証情報３３３を生成することができる。例えば、アプリケーション３２０およびホットスポットＢ　３２４のアプリケーション層３２９は、アプリケーション層で逆ブートストラップ手順を行うことができ、それによりユーザ／装置３２１および／またはホットスポットＢ　３２４がアクセス層の認証情報３３３を作成することが可能になる。したがって、アクセス層の認証情報３３３は、３１６で行われるアプリケーション層の認証手順の副産物と言える。これらのアクセス層の認証情報３３３は、装置３２１のアクセス層モジュール３２２および／またはホットスポットＢ　３２４のアクセス層３２８に送信することができる。呼び出しフロー３１８および３１９で、アプリケーション層で生成されたアクセス層の認証情報３３３を使用して、装置３２１およびホットスポットＢ　３２４は認証を行い、通信のためにアクセス層のセキュアな関連付けを設定することができる。認証後、アクセス層の認証情報３３３は、ユーザ／装置３２１が後にアクセス層３２８でホットスポットＢ　３２４への認証を試みる時に記憶するか、および／またはユーザ／装置３２１に関連付けることができる。

【００７５】

一実施形態によると、モバイル装置３２１を持つユーザは、ＭＮＯ　Ａ３２３に接続することができる。ユーザは、例えば映像サービス提供者などのサービス提供者に対してブートストラップ認証手順で認証することができる。この認証では、図３の３０７に示すように認証情報がブートストラップされる限り、当業者に知られる任意の各種技術を使用して、装置３２１にある事前に供給されたアクセス層の認証情報３３０を使用することができ、それによりアプリケーション層の識別を一意にネットワーク識別に関連付けることができる。ＭＮＯ　Ａ　３２３はＯｐｅｎＩＤプロバイダとして機能することができる。ホットスポットＢ　３２４はリライングパーティ（ＲＰ）として機能することができる。例示的実施形態によると、例えば映像サービス提供者からの映像を閲覧するなどのサービスにアクセスしている間に、ユーザがホットスポットＢの範囲内に移動する可能性がある。ネットワークホットスポットＢは、例えば、より高い帯域幅をより低い費用で提供する、および／または例えばＯｐｅｎＩＤネットワークと提携している（または例えばＭＮＯ　Ａ　３２３もしくは別のＭＮＯに関連付けられている）ような場合がある。ユーザは、原則として、提携しているＯｐｅｎＩＤネットワーク（または関連付けられたＭＮＯ　Ａ　３２３）へのアクセスを許可される。例えば、ユーザは、自身が、ＯｐｅｎＩＤプロバイダのＭＮＯ　Ａ　３２３に関連付けられていることを証明することができる。

【００７６】

装置３２１は、例えばビーコンおよび／または同報通信メッセージを監視する等により、後続ネットワークのホットスポットＢ　３２４を発見する、および／または後続ネットワークについての情報を把握することができる。情報は、例えば接続マネジャ（ＣＭ）を通じてアクセス層モジュール３２２からアプリケーション３２０に渡すことができ、アプ

リケーション３２０はその情報を使用して、ユーザ／装置３２１のアプリケーション層識別を用いてアプリケーション層３２９でホットスポットＢ　３２４に接触することができる。装置３２１は、アクセス層３２２および３２８を通じてホットスポットＢ　３２４に識別情報を送信することができる。

【００７７】

アプリケーション層３２９ではなく、アクセス層３２８を介して識別情報が通信されると、ユーザ／装置３２１の識別情報を、例えば３１４に示すようにホットスポットＢ　３２４のアプリケーションまで渡すことができる。ホットスポットＢ　３２４は、ＯｐｅｎＩＤに基づくＭＮＯ　Ａ　３２３の発見に適するようにその情報をフォーマットすることができる。識別情報は、３１６でホットスポットＢ　３２４がＭＮＯ　Ａ　３２３を発見する、および／または要求しているユーザ／装置３２１の認証を試みるのに十分である可能性がある。ホットスポットＢ　３２４は、例えばリライングパーティとして機能することができ、ＯｐｅｎＩＤプロトコルを実行してユーザ／装置をリダイレクトして、ＭＮＯ　Ａ　３２３で認証させることができる。ＭＮＯ　Ａ　３２３は、例えばＯｐｅｎＩＤサーバとして機能することができ、ＯｐｅｎＩＤプロトコルを実行してユーザ／装置３２１を認証することができる。ユーザ／装置３２１の認証が成功すると、ホットスポットＢ　３２４は、３１９で装置３２１とネットワークとの間にセキュアな接続を確立することができる。

【００７８】

ホットスポットＢ　３２４およびユーザ／装置３２１は、成功したＯｐｅｎＩＤに基づく認証に基づいて共有認証情報を作成することができる。例えば、ユーザ／装置３２１および／またはホットスポットＢ　３２４は、後続アクセス層の認証情報３３３を逆ブートストラップすることができる。ホットスポットＢ　３２４とＭＮＯ　Ａ　３２３との間の関係に基づいて何らかの発見を行うことができる。この情報は、ユーザ／装置３２１のアプリケーション層識別および／または装置３２１のアプリケーション３２０から得られる発見されたホットスポットＢ　３２４の情報を介して取得することができる。ユーザ／装置３２１がＭＮＯ　Ａ　３２３に認証されると、ホットスポットＢ　３２４のアプリケーションからホットスポットＢ　３２４のアクセスネットワークへの認証情報の（逆）ブートストラップを通じて、装置３２１とネットワークとの間にセキュアな接続を確立することができる。

【００７９】

一実施形態によると、ホットスポットＢ　３２４がアプリケーション層の認証情報３３１からアクセス層の認証情報３３３を逆ブートストラップするために、ホットスポットＢ　３２４は、層間通信およびデータ操作／処理が可能となり、および／または層間に関係が存在するようにアクセス層の機能とアプリケーション層の機能とが設計される能力を有することができる。逆ブートストラップはユーザに対してシームレスに行うことができ、後続のネットワークホットスポットＢ　３２４のための認証情報３３２を装置３２１に事前に供給もしくはインストールする必要がなく、および／または人的介在は必要とされない。

【００８０】

後続ネットワークのアクセス層で認証を行うための本明細書に記載される実施形態は、ユーザレベルで顕著な特性を有することができる。例えば、ユーザは、ユーザまたは装置の識別子（例えば、ＯｐｅｎＩＤ識別子）を入力してサービスにログオンすることができ、ユーザは、事前に未知であったアクセスネットワーク（例えばホットスポットＢ　３２４）にアクセスすることができ、その間サービスはシームレスに中断のない状態を保つことができる。例えばアクセス層の認証情報３３３などの認証の認証情報は、後続ネットワークで事前に供給されなくてよい。これは、すでに実行されているアプリケーションサービスセキュリティまたはアプリケーション層の認証から認証の認証情報を逆ブートストラップできるためである。サービスは、固定線および／またはワイヤレスである。サービスは、さらに、例えば公衆のインターネットおよび／または同様のアクセス手段を介して到

達可能な、ユーザの自宅にある独立したアクセスポイント（ＡＰ）であってもよい。

【００８１】

一実施形態によると、ハンドオフ（例えば、アクセス層のハンドオフ）の後にアプリケーション層のセキュリティを再度確立すべき場合は順方向の（forward）ブートストラップを使用することができる。順方向ブートストラップでは、そのような後続のアプリケーション層の認証のためのセキュリティ認証情報を、様々な以前の事例で確立されたセキュリティ認証情報（例えば、ハンドオフアクセス層の認証で使用された認証情報、以前のアプリケーション層の認証で使用された認証情報、またはさらにはハンドオフ以前にアクセス層の認証で使用された認証情報）に結び付ける。

【００８２】

本明細書に記載される実施形態では、独立した識別プロバイダを使用することができる。例えば、ＭＮＯ　Ａ　３２３がＯｐｅｎＩＤ識別プロバイダでなくてよく、および／または識別管理機能は別の第３者によって行われてもよい。第３者の識別プロバイダは、事前に確立されたＭＮＯ　Ａ　３２３との関係を使用してＯｐｅｎＩＤプロバイダの役割を果たし、例えばＯｐｅｎＩＤ／ＥＡＰ－ＳＩＭやＯｐｅｎＩＤ／ＧＢＡのブートストラップ能力などのプロトコルを使用して、ＭＮＯ　Ａ　３２３から供給されたアクセス層の認証情報３３０からアプリケーション層の認証情報３３１を認証およびブートストラップすることができる。それと同じまたは同様のブートストラップ処理を後に使用して、装置３２１上にあるＭＮＯ　Ａ　３２３から供給された認証情報を利用して、ホットスポットＢ　３２４のためのアクセス層の認証情報３３３をブートストラップすることができる。

【００８３】

別の実施形態によると、ネットワーク主導のハンドオフを実装することができる。ネットワーク主導のハンドオフでは、ハンドオフは、例えばアクセスネットワークやアプリケーションサーバなどのネットワークによって開始することができる。一例では、ＭＮＯ　Ａ　３２３が継続的に装置３２１を監視することができ、監視内容は、装置のある場所、測定情報、サービス品質等の情報を含むことができる。ＭＮＯ　Ａ　３２３は、装置３２１周辺のローカル環境を把握することができる。ＭＮＯ　Ａ　３２３がＯｐｅｎＩＤプロバイダでもある場合は、ＭＮＯ　Ａ　３２３は、装置３２１がハンドオフを発見および開始できるようにする適切なパラメータと共に、アプリケーション層でユーザ／装置にメッセージを送信して、ホットスポットＢ　３２４とのハンドオフを行わせることができる。シームレスなハンドオフを本明細書に記載されるように行うことができる。別の実施形態では、ＭＮＯ　Ａ　３２３は、装置３２１とのアクセス層の通信を介して、装置３２１にハンドオフのトリガ情報を送信することができる。

【００８４】

別の実施形態によると、ＭＮＯ　Ａ　３２３は、近くのローカルアクセスノードに要求を発行して、装置がそのノードの範囲内にある時に、装置３２１のアタッチおよび／または認証を試みることができる。ハンドオフをトリガするのはＭＮＯ　Ａ　３２３でなくともよい。装置３２１についての十分な情報を持つ任意のネットワーク構成要素、装置のローカルな通信環境、および／またはユーザ／装置３２１と通信する能力を持つエンティティがハンドオフをトリガできる場合がある。そのような場合、ネットワーク構成要素は、後続のアクセスネットワーク（例えば、ホットスポットＢ　３２４）を発見し、および／または、ユーザ／装置３２１と通信するためのセキュリティ能力および無線アクセス能力を取り決めることができる。ネットワーク構成要素は、その情報とハンドオフ情報をユーザ／装置３２１に通信することができる。

【００８５】

別の実施形態によると、アプリケーションで支援された認証情報のブートストラップを行うことができる。アプリケーションで支援された認証情報のブートストラップでは、装置３２１のアプリケーション３２０が、アプリケーションサーバ３２５が、ハンドオフを容易にするアプリケーション３２０の助けを借りて、後続のアクセスネットワークのホットスポットＢ　３２４のための認証情報のセットをブートストラップできることをアプリ

ケーションサーバ３２５に通知することができる。アプリケーション３２０は、発見されたホットスポットＢ　３２４に関連する識別、例えばＩＰアドレス、および任意でＯｐｅｎＩＤログインに類似する要求をアプリケーションサーバ３２５に送信することができる。アプリケーションサーバ３２５は、ＯｐｅｎＩＤプロバイダのように機能して、ホットスポットＢ　３２４のセキュリティ能力を取り決めることができる。アプリケーションサーバ３２５は、アクセス層でのホットスポットＢ　３２４および装置３２１のためのアクセス層の認証情報のセット３３３を逆ブートストラップすることができる。装置３２１のアプリケーション３２０とホットスポットＢ　３２４は、３１８に示すように互いを認証し、および／またはセキュアなチャネルを確立することができる。アプリケーションサーバ３２５と対象ホットスポットＢ　３２４との間の関係に基づいて何らかの発見を行うことができる。この情報は、装置３２１のアプリケーション３２０からの発見された情報を介して取得することができる。

【００８６】

後に発見されるネットワークの認証のための認証情報は、両終端点で事前に処理して、後の認証手順をより迅速に完了できるようにすることができる。これは、ネットワークが、装置が位置するローカルエリア、または装置が移動して向かっている先のローカルエリアを把握しているという知識に基づくことができる。装置がハンドオフの機会を探すように事前に構成されている場合、装置は、何らかの周期的な頻度で代替ネットワークを探し、検出された場合はハンドオフを要求することができる。ネットワーク側の事前処理は、２つ以上の代替アクセスノードで、またはそのようなノードに対して実施することができる。装置および／またはネットワークは、以前に使用したネットワークに使用した認証情報をキャッシュしておくことができる。装置および／またはネットワークは後にそれらの認証情報を認証に再使用することができる。この認証情報の再使用は、例えば装置が以前に離れたノードに戻る時に有用である場合がある。認証情報の再使用は、１つまたは複数のノードを代替的に動的に選択する場合も有用である場合がある（例えば、局所的に動的に変化する雑音のあるチャネルや品質のサービス環境などで）。

【００８７】

本明細書に記載される実施形態は、ローカルのＯｐｅｎＩＤを使用することができる。例えば、独立型のローカルＯｐｅｎＩＤを実装することができる。本明細書に記載されるように、プロトコルフローは、ローカルＯｐｅｎＩＤを利用し、アクセス権／権限を付与することができる。

【００８８】

図４は、独立型のローカルＯｐｅｎＩＤを使用したプロトコルの実現を説明する流れ図である。図４に示すように、流れ図は、ローカルＩｄＰ４３２、アプリケーション４３３（例えばブラウジングエージェント）、アクセス層モジュール４３４、ＭＮＯ４３５、ホットスポット４３６、および／またはアプリケーションサーバ４３７間の通信を含むことができる。ローカルＩｄＰ４３２は、ユーザのワイヤレス通信装置に配置することができる。アプリケーション４３３および／またはアクセス層モジュール４３４は、ローカルＩｄＰ　４３２と同じワイヤレス通信装置に配置しても、異なるワイヤレス通信装置に配置してもよい。

【００８９】

図４に示すプロトコルは、シームレスなハンドオフおよび／または後続のアクセス層のセキュリティの関連付けの設定を可能にする。このプロトコルは、例えばクライアントのローカルにあるＯｐｅｎＩＤ（すなわちローカルＯｐｅｎＩＤ）プロトコルを使用する等により、装置と装置の現在のアクセス層ネットワークとの間のアクセス層のセキュリティ、および／またはユーザ／装置と外部のアプリケーションサーバ（ＡＳ）４３７との間に以前に確立されたアプリケーションセキュリティを実装することができる。

【００９０】

図４に示すように、装置は、ステップ４０１～４１９の組合せを使用してアプリケーションサーバ（ＡＳ）／ＲＰ４３７との間でアプリケーション層で認証されることができ、

装置は、ステップ４１９～４３１の組合せを使用してアクセス層で後続ネットワーク（例えば、ホットスポット４３６）に対して認証されることができる。４０１で、装置のアクセス層モジュール４３４がＭＮＯ４３５にアタッチすることができる。装置のアクセス層モジュール４３４およびＭＮＯ４３５は、共有認証情報を使用して認証を行うことができる。認証の結果、アクセス層鍵Ｋを、装置のアクセス層モジュール４３４および／またはＭＮＯ４３５で確立することができる。４０２で、アクセス層鍵Ｋを装置に記憶することができる。例えば、アクセス層鍵Ｋは、例えば加入者識別モジュール（ＳＩＭ）カード、汎用集積回路カード（ＵＩＣＣ）、トラステッドプラットフォームモジュール（ＴＰＭ）、または他の高信頼環境などの装置上の高信頼環境に記憶することができる。高信頼環境は、装置に含まれても、または例えば別個のモジュールや別個の装置／機器として装置に接続されてもよい。高信頼環境はローカルＩｄＰ４３２を含むことができる。例示的実施形態によると、高信頼環境とローカルＩｄＰ４３２は同一のエンティティとすることができる。ただし、高信頼環境は、例えば、アプリケーション４３３、アクセス層モジュール４３４、および／または装置に位置する他のエンティティも含むことができる。

【００９１】

４０３で、ＭＮＯ４３５と装置のアクセス層モジュール４３４との両方がアクセス層鍵Ｋからアプリケーション層鍵Ｋ＿ａｐｐを導出することができる（すなわちＫ＿ａｐｐ＝ｆ（Ｋ）。ｆは、ＭＮＯ４３５と装置のアクセス層モジュール４３４との両方に知られている何らかの関数）。アプリケーション層鍵Ｋ＿ａｐｐは、ローカルＩｄＰ４３２が入手可能な状態にされる。４０４で、アクセス層鍵Ｋを使用して、アクセス層のセキュリティの関連付けが装置のアクセス層モジュール４３４とＭＮＯ４３５との間に確立される。

【００９２】

４０５で、ユーザがアプリケーション４３３を介してアプリケーションサーバ（ＡＳ）４３７にログインすることができる。ユーザは、例えばＯｐｅｎＩＤプロバイダ（ＯＰ）識別子（例えば、ＵＲＬまたは電子メールアドレス）を用いてログインすることができる。ＡＳ４３７はリライングパーティ（ＲＰ）として機能することができ、したがって本明細書ではＡＳ／ＲＰ４３７と呼ぶことができる。４０６で、ＡＳ／ＲＰ４３７は　ＭＮＯ４３５の識別の発見を行うことができる。４０７で、ＭＮＯ４３５とＡＳ／ＲＰ４３７間の関連付けを設定し、関連付けハンドルを生成することができる。ＭＮＯ４３５は、４０８で、アプリケーション鍵Ｋ＿ａｐｐおよび関連付けハンドルからセッション鍵Ｋ＿ｓｅｓｓｉｏｎを導出することができる。４０９で、関連付けセキュリティプロトコルを使用してＫ＿ｓｅｓｓｓｉｏｎをＡＳ／ＲＰ４３７に渡し、Ｋ＿ｓｅｓｓｉｏｎを以後の関連付け鍵として使用することができる。４１０で、ＡＳ／ＲＰ４３７は、セッション鍵Ｋ＿ｓｅｓｓｉｏｎおよび以後の関連付け情報を記憶することができる。４１１で、アプリケーション４３３は装置でリダイレクトされて、ローカルＩｄＰ４３２に対して認証することができる。リダイレクトメッセージは、セッションノンスおよび／または関連付けハンドルを含むことができる。４１２で、アプリケーション４３３は、カードアクセス層モジュール４３４を通じてローカルＩｄＰ４３２への接続を要求することができる。この要求は、例えばセッションノンスおよび／または関連付けハンドルを含むことができる。４１３で、ローカルＩｄＰ４３２へのリダイレクトを行うことができる。このリダイレクトも、セッションノンスおよび／または関連付けハンドルを含むことができる。４１４で、ローカルＩｄＰ４３２は、アプリケーション層鍵Ｋ＿ａｐｐおよび関連付けハンドルを使用して署名鍵Ｋ＿ｓｅｓｓｉｏｎを導出することができる。ローカルＩｄＰ４３２は、装置にあるアプリケーション層鍵Ｋ＿ａｐｐにアクセスすることができる。ローカルＩｄＰ４３２は、４１５でＯｐｅｎＩＤのアサーションメッセージを作成し、Ｋ＿ｓｅｓｓｉｏｎを使用してそれに署名することができる。４１６で、ローカルＩｄＰ４３２は、署名したＯｐｅｎＩＤアサーションメッセージをリダイレクトして、カードアクセスを通じて装置のアクセス層モジュール４３４に戻すことができる。装置のアクセス層モジュール４３４は、４１７で、署名済みのＯｐｅｎＩＤアサーションを透過に装置のアプリケーション４３３にリダイレクトすることができる。装置のアプリケーション４３３は、４１８で署名

済みのＯｐｅｎＩＤアサーションメッセージを、ステップ４１１で受け取ったノンスと共に外部のＡＳ／ＲＰ４３７にリダイレクトすることができる。４１９で、ＡＳ／ＲＰ４３７は、受信した署名済みのアサーションメッセージを記憶することができる。

【００９３】

装置がアプリケーション層でＡＳ／ＲＰ４３７に対して認証されると、装置は、アプリケーション層の認証からの認証情報または鍵を使用して、アクセス層で後続ネットワーク（例えば、ホットスポット４３６）に対して認証することができる。図４に示すように、４２０で、装置のアクセス層モジュール４３４はホットスポット４３６を発見することができる。装置のローカルエンティティ（例えば、接続マネジャ（ＣＭ））が、装置が発見されたホットスポット４３６に切り替わるべきであると判断することができる。４２１で、装置のアクセス層モジュール４３４がホットスポット４３６の情報を装置のアプリケーション４３３に渡すことができる。４２２で、装置のアプリケーション４３３がＯｐｅｎＩＤ識別子（例えば、ＵＲＬまたは電子メールアドレス）を、前回使用されたアプリケーションサーバ４３７の識別と共に、後の発見のためにホットスポット４３６のアクセス層に渡すことができる。４２３で、装置のアプリケーション４３３は、ハンドオフの開始をＡＳ／ＲＰ４３７に通知することができる。４２３のハンドオフの初期化は、発見されたホットスポット４３６の情報を使用して行うことができる。装置のアプリケーション４３３は、４１８で確立された自身のアプリケーション層の識別および／またはホットスポットＢ　４３６のアクセス層発見情報に基づいて、アクセス層の適切な識別を決定することができる。アクセス層の識別はアプリケーション層の識別に結び付けることができ、４２２で後の送信のためにアクセス層モジュール４３４に送信することができる。

【００９４】

図４のステップ４２４～４２９に示すように、ＡＳ／ＲＰ４３７は、装置のアクセス層の認証を容易にすることができる。例えば、ＡＳ／ＲＰ４３７は、アサーションメッセージをアクセス層モジュール４３４に転送することができる。ＭＮＯ４３５はアサーションを検証し、したがってアクセス層の識別を保証することができる。４２４で、装置のアクセス層モジュール４３４がホットスポット４３６にログイン要求を発行することができる。このメッセージに含まれるのは、例えば４２２で説明したＯｐｅｎＩＤ識別子（例えば、ＵＲＬまたは電子メールアドレス）、および／または前回アプリケーションサーバで使用された識別である。４２５で、ホットスポット４３６は、装置およびそのユーザの認証の情報をＡＳ／ＲＰ４３７に要求することができる。例えば、ホットスポット４３６は、装置のアクセス層４３４から受け取ったＯｐｅｎＩＤ識別子（例えば、ＵＲＬまたは電子メールアドレス）についてのアサーションを要求することができる。４２６で、ＡＳ／ＲＰ４３７は、ステップ４１８でＡＳ／ＲＰ４３７に受信され、ステップ４２５で受信されたＯｐｅｎＩＤ識別子に対応する署名済みのアサーションメッセージをホットスポット４３６に返すことができる。４２７で、ホットスポット４３６は、ＭＮＯ４３５のＯｐｅｎＩＤサービスに、ＯｐｅｎＩＤ識別子（例えば、ＵＲＬまたは電子メールアドレス）に対応する署名済みアサーションメッセージについて署名の検証を要求することができる。４２８で、ＭＮＯ４３５は、署名を（例えばＯｐｅｎＩＤサーバで）検証することができる。ＭＮＯ４３５は、ステップ４０８からセッション鍵Ｋ＿ｓｅｓｓｉｏｎを保持していることができる。ＭＮＯ４３５は、４２９で、署名検証メッセージを（例えば自身のＯｐｅｎＩＤサーバを使用して）ホットスポット４３６に提供することができる。

【００９５】

認証が成功した場合、ホットスポット４３６は、４３０で認証成功の肯定応答を装置のアクセス層モジュール４３４に送信することができる。装置のアクセス層モジュール４３４およびホットスポット４３６は、４３１で関連付けを設定して、両者の共通チャネルをセキュリティ保護することができる。対称鍵構造の導出で通信をセキュリティ保護することができる。図４に示すプロトコルのステップ４３１では、当業者に知られる各種の代替法を使用してアクセス層の鍵／認証情報を導出することができる。例えば、鍵導出機能を、署名の検証が済んだアプリケーション層のアサーションメッセージに使用することがで

きる。

【００９６】

逆ブートストラップの実装は、本明細書に記載されるように明示的であっても暗黙的であってもよい。例えば、図４に示すプロトコルでは逆ブートストラップを暗黙的に実装することができる。アクセス層のセキュリティの関連付けがアプリケーション層から提供されるアサーションに基づいて確立されることが想定される場合は、例えばアクセス層鍵および／または認証情報を直接アプリケーション層の認証情報から明示的に導出するのではなく、逆ブートストラップは暗黙的に行うことができる。明示的な逆ブートストラップは、アクセス層鍵が、例えばアプリケーション層の認証情報から直接の逆ブートストラップの明示的なプロセスを介して導出される場合に行うことができる。

【００９７】

別の実施形態によると、プロトコルで、アクセス権／権限も付与するシームレスなハンドオフを可能にすることができる。例えば、図５は、アクセス権／権限も付与する、暗黙的な逆ブートストラップを使用したシームレスなハンドオフを可能にするプロトコルを説明する流れ図である。図５に示すプロトコルを使用すると、ホットスポット５３６が、例えばサービスにアクセスするためのアクセス層のハンドオフおよび権限、またはユーザのプライベートデータを得られるようにすることができる。

【００９８】

図５に示すように、５０１で、装置のアクセス層モジュール５３４は、例えばアクセス層でＭＮＯ５３５にアタッチすることができる。装置のアクセス層モジュール５３４およびＭＮＯ５３５は、共有認証情報を使用して相互認証を行うことができる。共有認証情報は、例えばアクセス層の共有認証情報である。認証の結果、アクセス層鍵Ｋを、装置のアクセス層モジュール５３４と、ＭＮＯ５３５、例えばＭＮＯのアクセス層との両方で確立することができる。５０２で、アクセス層鍵Ｋを装置に記憶することができる。例えば、アクセス層鍵Ｋは装置上の高信頼環境に記憶することができる。高信頼環境は、装置に含まれても、または例えば別個のモジュールや別個の装置／機器として装置に接続されてもよい。高信頼環境はローカルＩｄＰ５３２の機能を有することができる。高信頼環境は、図５に示すようにローカルＩｄＰ５３２と同じエンティティであってもよい。

【００９９】

５０３で、ＭＮＯ５３５および／または装置のアクセス層モジュール５３４がアクセス層鍵Ｋからアプリケーション層鍵Ｋ＿ａｐｐを導出することができ（すなわちＫ＿ａｐｐ＝ｆ（Ｋ）。ｆは、ＭＮＯ５３５と装置のアクセス層５３４の両方に知られている何らかの関数）、Ｋ＿ａｐｐをローカルＩｄＰ５３２が入手可能な状態にすることができる。５０４で、Ｋ＿ａｐｐを使用して、アクセス層の関連付けを装置のアクセス層モジュール５３４とＭＮＯ５３５との間に確立することができる。５０５で、ユーザがアプリケーション５３３を介してアプリケーション層でＡＳ／ＲＰ５３７にログインすることができる。例えばユーザはＯＰ識別子（例えば、ＵＲＬまたは電子メールアドレス）を用いてログインすることができる。５０６で、ＡＳ／ＲＰ５３７はＭＮＯ５３５の発見を行うことができる。５０７で、ＭＮＯ５３５とＡＳ／ＲＰ５３７間の関連付けを設定し、関連付けハンドルを生成することができる。５０８で、ＭＮＯ５３５は、Ｋ＿ａｐｐおよび関連付けハンドルからＫ＿ｓｅｓｓｉｏｎを導出することができる。５０９で、例えば元の関連付けセキュリティおよびＫ＿ｓｅｓｓｉｏｎを以後の関連付け鍵として使用することにより、Ｋ＿ｓｅｓｓｓｉｏｎをＡＳ／ＲＰ５３７に渡すことができる。５１０で、ＡＳ／ＲＰ５３７はＫ＿ｓｅｓｓｉｏｎおよび後続の関連付け情報を記憶することができる。５１１で、アプリケーション５３３（例えば、ＢＡ）をＡＳ／ＲＰ５３７により装置上でリダイレクトして、ローカルＩｄＰ５３２に対して認証させることができる。メッセージは、ノンスおよび／または関連付けハンドルを含むことができる。５１２で、アプリケーション５３３が、アクセス層５３４を通じてローカルＩｄＰ５３２への接続を要求することができる。この要求はノンスおよび／または関連付けハンドルを含むことができる。５１３で、ローカルＩｄＰ５３２へのリダイレクトが行われる。リダイレクトメッセージもノンスお

よび／または関連付けハンドルを含むことができる。

【０１００】

５１４で、ローカルＩｄＰ５３２は、Ｋ＿ａｐｐおよび関連付けハンドルを使用して署名鍵Ｋ＿ｓｅｓｓｉｏｎ（例えば、アサーションメッセージを署名するため）を導出することができる。ローカルＩｄＰ５３２は、Ｋ＿ａｐｐにアクセスできる可能性がある。５１５で、ローカルＩｄＰ５３２はＯｐｅｎＩＤアサーションメッセージを作成し、Ｋ＿ｓｅｓｓｉｏｎを使用してアサーションメッセージに署名することができる。５１６で、ローカルに生成されたアクセス／権限付与トークンの提供元として機能するローカルＩｄＰ５３２が署名鍵Ｋ＿ｔｏｋｅｎを導出することができる。署名鍵Ｋ＿ｔｏｋｅｎは後にアクセス／権限付与トークンに署名するために使用することができる。そのようなＫ＿ｔｏｋｅｎを導出する方式の１つは、Ｋ＿ａｐｐとＫ＿ｓｅｓｓｉｏｎの両方を入力とする鍵生成機能（ＫＧＦ）を使用するものである。例えば、Ｋ＿ｔｏｋｅｎ＝ｆ（Ｋ＿ａｐｐ，Ｋ＿ｓｅｓｓｉｏｎ）である。５１７で、ローカルに生成されたアクセス／権限付与トークンの提供元として機能するローカルＩｄＰ５３２がアクセス／権限付与トークンを作成し、および／またはＫ＿ｔｏｋｅｎでトークンに署名することができる。５１８で、ローカルＩｄＰ５３２は、署名したアサーション（署名済みＯｐｅｎＩＤアサーションおよび署名済みアクセス／権限付与トークンの両方）をリダイレクトしてアクセス層５３４（例えば、カードアクセス）を通じて装置のアクセス層に戻すことができる。５１９で、装置のアクセス層５３４は、署名したアサーション（ＯｐｅｎＩＤアサーションおよびアクセス／権限付与トークン）を装置のアプリケーション５３３にリダイレクトすることができる（透過なリダイレクトで）。５２０で、装置のアプリケーション（例えば、ＢＡ）が、署名したアサーション（ＯｐｅｎＩＤアサーションおよびアクセス／権限付与トークン）を、５１１で受け取ったノンスと共に外部のアプリケーションＡＳ／ＲＰ５３７にリダイレクトすることができる。ＡＳ／ＲＰ５３７は、受け取った署名済みアサーションメッセージを記憶することができる。

【０１０１】

５２１で、装置は、自身のアクセス層モジュール５３４を介してホットスポット５３６を発見することができる。装置の接続マネジャ（ＣＭ）は、装置が発見されたホットスポット５３６に切り替わるべきと判断することができる。５２２で、装置のアクセス層モジュール５３４は後続ホットスポットの情報を装置のアプリケーション５３３に渡すことができる。５２３で、装置のアプリケーション５３３は、ＯｐｅｎＩＤ識別子を、前回使用されたアプリケーションサーバ識別と共にホットスポット５３６のアクセス層に渡すことができる。装置のアプリケーション５３３は、５２４で、発見されたホットスポット５３６へのハンドオフの開始をＡＳ／ＲＰ５３７に通知することができる。これは、装置のアクセス層モジュール５３４が、例えばホットスポット５３６にログイン要求を送信することによって行うことができる。このメッセージには、ＯｐｅｎＩＤ識別子および／またはアクセストークンを含めることができる。アプリケーション５３３は、このトークンをステップ５１９から保持していることができる。５２５で、ホットスポット５３６は、ＭＮＯ５３５のＯｐｅｎＩＤ／ＯＡｕｔｈサーバを発見することができる。５２６で、ホットスポット５３６は、ＭＮＯ５３５のＯｐｅｎＩＤ／ＯＡｕｔｈサーバに、ＯｐｅｎＩＤ識別子および／または署名済みアクセストークンを使用してユーザ／装置を認証し、アクセスを許可するように要求することができる。５２７で、ＭＮＯ５３５のＯｐｅｎＩＤ／ＯＡｕｔｈサーバは署名鍵Ｋ＿ｔｏｋｅｎを計算することができる。署名鍵Ｋ＿ｔｏｋｅｎは、例えばステップ５１６でＫ＿ｔｏｋｅｎが計算されたとの同じ方式で計算することができる。５２８で、ＭＮＯ５３５のＯｐｅｎＩＤ／ＯＡｕｔｈサーバは、ステップ５２７で計算したＫ＿ｔｏｋｅｎを使用して、受け取ったアクセストークンの署名を検証することができる。５２９で、ＭＮＯ５３５のＯｐｅｎＩＤ／ＯＡｕｔｈサーバは、アクセストークンの肯定のアサーションを、ユーザ／装置の任意の追加的な識別情報と共にホットスポットに送信することができる。５３０で、認証が成功した場合、ホットスポット５３６は、アクセス層モジュール５３４で装置に認証成功の肯定応答を送信することができる。

５３１で、装置５３１のアクセス層モジュール５３４およびホットスポット５３６は、セキュリティの関連付けを相互に設定することができる。その後に鍵の導出および／またはセキュアな通信が行われることができる。

【０１０２】

本明細書に記載されるように、アプリケーション層の認証情報を使用して、本明細書に記載されるように、ユニバーサルアクセス方法（ＵＡＭ）および／または拡張可能認証プロトコル（ＥＡＰ）を利用した公衆のホットスポットにおける後のアクセス層またはＩＰ層の認証で使用される認証情報を生成することができる。

【０１０３】

ＯｐｅｎＩＤとＵＡＭを利用する公衆のホットスポットとを統合するための実装の選択肢は、種々のネットワークエンティティがリライングパーティ（ＲＰ）またはＯｐｅｎＩＤプロバイダ（ＯＰ）として機能する各種実装を含むことができる。例えば、ホットスポットの認証、認可および課金（ＡＡＡ）サーバがＲＰとして機能する、ホットスポットのワイヤレスローカルエリアネットワーク（ＷＬＡＮ）ゲートウェイがＲＰとして機能する、ホットスポットのキャプティブポータルがＲＰとして機能する、ホットスポットアクセスポイント（ＡＰ）がＲＰとして機能する（例えばカフェで使用されるホットスポットなど小さなホットスポットの場合）、および／またはホットスポットのＡＡＡサーバがＯＰとして機能する等が可能である。ＲＰ機能を実装するホットスポットのＡＡＡサーバおよびＷＬＡＮゲートウェイを使用する、ＯｐｅｎＩＤとＵＡＭの統合の例示的実施形態を図６および図７に説明することができる。他の実施形態も実装は同様であるが、異なる展開モデルを有することが理解されよう。

【０１０４】

例示的実施形態によると、モバイル装置を持つユーザが、ＯＰサーバとして機能するＭＮＯ　Ａに接続することができる。ユーザは、装置上の事前に供給されたアクセス層の認証情報を使用して、ブートストラップ認証手順でサービスに対して認証することができる。ブートストラップ認証手順は、アプリケーション層識別を一意にネットワーク識別に関連付けることができる。例として、認証はＯｐｅｎＩＤを使用して行うことができるが、任意の他の同様の認証プロトコルを使用してもよい。ＯｐｅｎＩＤが実装されている場合、ＭＮＯ　ＡはＯｐｅｎＩＤプロバイダとして機能し、および／または、ホットスポットＢのＷＬＡＮゲートウェイがリライングパーティとして機能することができる。

【０１０５】

装置は、ＭＮＯ　Ａに接続すると、別のネットワークを（例えば、ビーコンまたは同報通信メッセージを監視することにより）発見する、および／またはアクセス層で新たに発見したネットワークについての情報を把握することができる。この情報は、例えば接続マネジャ（ＣＭ）を通じて、装置上のアプリケーションに渡すことができる。装置のアプリケーションは、発見されたネットワークに関する情報を使用して、ユーザ／装置の識別を用いてアプリケーション層でホットスポットＢのＷＬＡＮゲートウェイに接触することができる。この識別情報は、図６に示すようにＲＰとして機能するＡＡＡサーバおよび／または図７に示すようにＲＰとして機能するＷＬＡＮゲートウェイがＭＮＯ　Ａを発見し、要求元のユーザ／装置の認証を試みるのに十分である可能性がある。ＯＰ←→ＲＰプロトコルを、ＭＮＯ　Ａ（ＯｐｅｎＩＤサーバとして機能する）と、ホットスポットＢのＷＬＡＮゲートウェイまたはＡＡＡサーバ（リライングパーティとして機能する）の少なくとも一方とによって実行して、ユーザ／装置を認証することができる。ユーザ／装置の認証が成功すると、ユーザ／装置はホットスポットＢへのアクセスを許可されることができる。例えば、図６では、ＡＡＡサーバがユーザを認証し、認証成功の通知（アクセス受付けメッセージ）をホットスポットＢのＷＬＡＮゲートウェイに送信すると、ユーザのホットスポットＢへのアクセスを許可することができる。同様に、図７では、ホットスポットＢのＷＬＡＮゲートウェイがユーザ／装置を認証すると、ユーザ／装置のホットスポットＢへのアクセスを許可することができる。この認証は、ユーザに対してシームレスに、および／または後に発見されるネットワーク（ホットスポットＢ）のための認証情報を装置に

事前に供給またはインストールする必要なしに、または人的介在を必要とせずに行うことができる。

【０１０６】

図６は、ＲＰとして機能するＡＡＡサーバ６１７を使用する、ＵＡＭとＯｐｅｎＩＤの統合を説明する流れ図である。図６に示すように、ＵＥ６１４、ＡＰ６１５、ＷＬＡＮ　ＧＷ　６１６、ＡＡＡサーバ／ＲＰ６１７、および／またはＯＰサーバ６１８が通信を行って、ＵＥ６１４がワイヤレスネットワークに対して認証することを可能にする。ＵＥ６１４のローカルコンポーネント（例えばＣＭ）が、ホットスポットの識別の情報（例えば「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤ）に基づいてホットスポットＡＰ６１５を発見することができる。識別の情報は、例えばビーコンチャネルなどのアクセス層のシグナリングを介して発見することができる。ＵＥ６１４のローカルコンポーネント（例えばＣＭ）は、ＵＥ６１４がそのホットスポットに切り替わるべきであると判断し、その指令をＵＥ６１４のアプリケーション層に伝えることができる。ＵＥ６１４のローカルコンポーネントは、アプリケーション層ネットワークの発見情報をＵＥ６１４のアプリケーション（例えばブラウザ）に送信することができる。

【０１０７】

図６に示すように、６０１で、ＵＥ６１４は、オープンモードのアクセスポイント（ＡＰ）６１５に関連付けることができる。例えば、ＵＥ６１４は、アクセス層で取得した識別の情報（例えば、「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤ）を使用してそのような関連付けおよび／またはオープンモードアクセスを行うことができる。ＵＥ６１４が（例えば、ＤＨＣＰを使用して）ＩＰアドレスを取得するように構成されている場合、ＷＬＡＮゲートウェイ（ＧＷ）６１６は、６０２でＵＥ６１４にプライベートＩＰアドレスを割り当てることができる。ＷＬＡＮ　ＧＷ６１６でＵＥ６１４の状態が「未許可」に設定されている場合があるため、ユーザは、そのプライベートＩＰアドレスを使用してインターネットにアクセスできない場合がある。

【０１０８】

ユーザは、ＵＥ６１４でウェブブラウザアプリケーションを開き、６０３でＷＬＡＮ　ＧＷ６１６がウェブページ（例えばユーザのホームページ）の要求をＵＥ６１４から受け取ることができる。ＷＬＡＮ　ＧＷ６１６は、６０４でＵＥ６１４のブラウザをポータルページ（例えばＩＰ／ＵＲＩ）にリダイレクトし、ポータルページがユーザにログイン認証情報を要求する。ユーザは自身のＯｐｅｎＩＤ識別子（例えば、ＵＲＬまたは電子メールアドレス）をログインページで入力することができる。６０５で、ＷＬＡＮ　ＧＷ６１６は、ＵＥ６１４からログイン認証情報を受け取り、ＷＬＡＮ　ＧＷ６１６は、受け取ったログイン認証情報を使用して、設定されたＡＡＡサーバ／ＲＰ６１７へのアクセス要求メッセージを生成することができる。ＷＬＡＮ　ＧＷ６１６は、６０６でアクセス要求メッセージをＡＡＡサーバ／ＲＰ６１７に送信することができる。

【０１０９】

ＲＰとして機能するＡＡＡサーバ６１７は、６０７でＯＰサーバ６１８の発見および／またはＯＰサーバ６１８との関連付けを行うことができる（例えばＯｐｅｎＩＤプロトコルを使用して）。６０８で、ＡＡＡサーバ／ＲＰ６１７は、ＵＥ６１４をＯＰサーバ６１８にリダイレクトすることができる。ＵＥ６１４は、６０９でＯＰサーバ６１８に対して認証することができる（例えばＯｐｅｎＩＤ認証情報を使用して）。ＯＰサーバ６１８は、６１０で、認証アサーションと共にＵＥ６１４をＡＡＡサーバ／ＲＰ６１７にリダイレクトすることができる。ＵＥ６１４は、６１１で、アサーションおよびＵＥ６１４が認証が成功した旨の通知をＡＡＡサーバ／ＲＰ６１７に提示することができる。

【０１１０】

６１２で、ＡＡＡサーバ／ＲＰは、認証成功の通知（例えばアクセス受付けメッセージ）をＷＬＡＮ　ＧＷ６１６に送信するか、および／またはＷＬＡＮ　ＧＷ６１６におけるユーザ／ＵＥ６１４のステータスを「許可」状態に変更する指示を送信することができる。ＷＬＡＮ　ＧＷ６１６は、６１３で、ユーザのブラウザを開始ページにリダイレクトし

、ユーザがＷＬＡＮネットワークを通じてインターネットにアクセスすることを可能にすることにより、ユーザ／ＵＥ６１４に認証成功を知らせることができる。

【０１１１】

ＯｐｅｎＩＤ　ＲＰ機能をＡＡＡサーバ６１７に組み込むことにより、ＡＡＡサーバ６１７は認証のためにＨＬＲ／ＨＳＳと通信せずに済む。また、ユーザは自身の認証情報をＷＬＡＮ　ＧＷ／ＲＰに送信せずに認証および／またはＷＬＡＮ　ＧＷ／ＲＰにアクセスすることができるため、ユーザ認証をセキュアにすることができる。

【０１１２】

図７は、ＲＰとして機能するＷＬＡＮ　ＧＷ７１４を使用する、ＵＡＭとＯｐｅｎＩＤとの統合を説明する流れ図である。図７に示すように、ＵＥ７１２、ＡＰ７１３、ＷＬＡＮ　ＧＷ／ＲＰ７１４、および／またはＯＰサーバ７１５が通信を行って、ＵＥ７１２がワイヤレスネットワークに認証してサービスにアクセスできるようにする。ＵＥ７１２のローカルコンポーネント（例えば、ＣＭ）が、ホットスポットの識別の情報（例えば、「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤ）に基づいてホットスポットＡＰ７１３を発見することができる。ＡＰ７１３は、例えばビーコンチャネルなどのアクセス層のシグナリングを介して発見することができる。ＵＥ７１２のローカルコンポーネント（例えばＣＭ）は、ＵＥ７１２がホットスポットＡＰ７１３に切り替わるべきであると判断し、その指令をＵＥ７１２のアプリケーション層に伝えることができる。ＵＥ７１２のローカルコンポーネントは、アプリケーション層ネットワークの発見情報をＵＥ７１２のアプリケーション（例えばブラウザ）に送信することができる。

【０１１３】

図７に示すように、７０１で、ＵＥ７１２は、オープンモードのアクセスポイント（ＡＰ）７１３に関連付けることができる。例えば、ＵＥ７１２は、「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤおよび／またはオープンモードアクセス使用してそのような関連付けを行うことができる。ＵＥ７１２がＤＨＣＰを使用してＩＰアドレスを取得するように構成されている場合、ＷＬＡＮ　ＧＷ／ＲＰ７１４が７０２でプライベートＩＰアドレスをＵＥ７１２に割り当てることができる。ユーザは、そのＩＰアドレスを使用してインターネットにアクセスできない場合がある。この時点で、ＷＬＡＮ　ＧＷ／ＲＰ７１４におけるＵＥ７１２の状態は「未許可」に設定されている場合があり、そのためＷＬＡＮ　ＧＷ／ＲＰ７１４を介してサービスにアクセスできない場合がある。

【０１１４】

ユーザは、ＵＥ７１２でウェブブラウザアプリケーションを開くことができる。７０３で、ＷＬＡＮ　ＧＷ／ＲＰ７１４は、ＵＥ７１２からウェブページ（例えばユーザのホームページ）の要求を受け取ることができる。ＷＬＡＮ　ＧＷ／ＲＰ７１４は、７０４でＵＥ７１２のブラウザをポータルページ（例えば、ＩＰ／ＵＲＩ）にリダイレクトし、ポータルページがユーザにログイン認証情報を要求する。ユーザは自身のＯｐｅｎＩＤ識別子（例えば、ＵＲＬまたは電子メールアドレス）をログインページで入力することができる。

【０１１５】

７０５で、ＷＬＡＮ　ＧＷ／ＲＰ７１４はＵＥ７１２からログイン認証情報を受け取り、ＷＬＡＮ　ＧＷ／ＲＰ７１４は、受け取ったログイン認証情報を使用してＯＰサーバ７１５の発見および／またはＯＰサーバ７１５との関連付けを行うことができる。７０６で、ＲＰとして機能するＷＬＡＮ　ＧＷ／ＲＰ７１４が（例えば、ＯｐｅｎＩＤプロトコルを使用して）ＯＰサーバ７１５の発見および／またはＯＰサーバ７１５との関連付けを行うことができる。ＷＬＡＮ　ＧＷ／ＲＰ７１４は、７０７でＵＥ７１２をＯＰサーバ７１５にリダイレクトすることができる。ＵＥ７１２は、７０８で（例えば、ＯｐｅｎＩＤ認証情報を使用して）ＯＰサーバ７１５に対して認証することができる。７０９で、ＯＰサーバ７１５は、ＵＥ７１２をＷＬＡＮ　ＧＷ／ＲＰ　７１４にリダイレクトすることができる。７０９のリダイレクトメッセージは認証アサーション情報を含むことができる。ＵＥ７１２は、７１０で、アサーション情報および／またはＯＰサーバ７１５への認証が成

功した旨の通知をＷＬＡＮ　ＧＷ／ＲＰ７１４に提示することができる。受け取ったアサーション情報および／または認証成功の通知に基づいて、ＷＬＡＮ　ＧＷ／ＲＰ７１４はユーザのステータスを「許可」状態に変更することができる。ＷＬＡＮ　ＧＷ／ＲＰ７１４は、ＵＥ７１２のブラウザを開始ページにリダイレクトすることによって認証の成功をユーザ／ＵＥ７１２に知らせ、ユーザはＷＬＡＮネットワークを通じてインターネットにアクセスすることができる。７１１で、ユーザ７１２がＷＬＡＮネットワークを通じてインターネットにアクセスできるようにすることができる。

【０１１６】

図７に示すようにＯｐｅｎＩＤのＲＰ機能をホットスポットのＷＬＡＮ　ＧＷ７１４に組み込むことにより、ＡＡＡサーバを認証のために使用せずに済む。ＷＬＡＮ　ＧＷ７１４はＲＡＤＩＵＳ機能を使用しなくてよい。図６に示す実施形態と同様に、図７の認証の実装は、ユーザが自身の認証情報をＷＬＡＮ　ＧＷ７１４に送信せずに認証および／またはホットスポットにアクセスすることができることから、セキュアな認証を含むことができる。図７に示す実装では、ＷＬＡＮサービス／ホットスポットの提供者は、認証が簡略化されるために、大きな顧客基盤に達することができる。例えば、１つのホットスポットで複数のＯＰに対応することができ、サービスを複数のＭＮＯ（例えばＯＰサーバ７１５として機能する）から顧客に提供することが可能となり、同時にＭＮＯにより提供される認証の基盤から利益を得ることができる。

【０１１７】

本明細書には、ＥＡＰを利用する公衆ホットスポットで後続のアクセス層またはＩＰ層の認証で使用するために、（例えば逆ブートストラップを使用して）アプリケーション層の認証情報から認証情報を生成する認証の実施形態も記載される。ユーザレベルでは、ユーザはＯｐｅｎＩＤ識別子を入力してサービスにログインし、例えばホットスポットＢなどの事前に未知であったアクセスネットワークにアクセスすることができ、その間サービスはシームレスに中断のない状態を保つことができる。アクセス層またはＩＰ層の認証情報は、すでに実行されているアプリケーションサービスセキュリティからブートストラップすることができるため、後続アクセスネットワークで事前に供給されなくてよい。

【０１１８】

ＥＡＰを利用した公衆ホットスポットを使用する認証の記載される実施形態は、ＯｐｅｎＩＤを組み込むための実装の選択肢を含むことができる。ＯｐｅｎＩＤと８０２．１ｘ／ＥＡＰの公衆ホットスポットを統合するための実装の選択肢は、ＲＰとして機能するホットスポットＡＡＡサーバの使用、ＯＰとして機能するホットスポットのＡＡＡサーバの使用、および／またはＥＡＰ－ＯｐｅｎＩＤの使用を含むことができる。

【０１１９】

図８は、ＲＰとして機能するＡＡＡサーバ８２０を使用する、ＥＡＰとＯｐｅｎＩＤとの統合を説明する流れ図である。ホットスポットのＡＡＡサービスにＲＰ機能を組み込むことにより、例えば３ＧＰＰネットワークとＷＬＡＮネットワーク間のシームレスな認証および／またはサービスの継続性の支援を可能にすることができる。ＵＥ８１８および／またはＯＰサーバ８２１で導出された鍵を利用してＥＡＰ－ＳＩＭ／ＡＫＡ認証を完了し、アクティブな接続（例えば、３ＧＰＰ接続）を使用してＯｐｅｎＩＤ認証を交換し、および／またはホットスポットＡＰ８１９がＵＥとＯｐｅｎＩＤの交換を行えるようにすることにより、ユーザは、ＡＡＡサーバ８２０にＲＰモジュールを組み込んだ公衆のホットスポットでシームレスに認証されることができる。

【０１２０】

図８に示すように、ＵＥ８１８および／またはそのユーザは、ＵＥ８１８、ＡＰ８１９、ＡＡＡ／ＲＰサーバ８２０、および／またはＯＰサーバ８２１間の通信を使用して認証することができる。ＵＥ８１８、ＡＡＡ／ＲＰサーバ８２０、および／またはＯＰサーバ８２１は各々、アプリケーション層で通信することが可能なアプリケーションを含むことができる。ＵＥ８１８、ＡＰ８１９、および／またはＡＡＡ／ＲＰサーバ８２０は各々、ＩＰ層の通信が可能なＩＰ層通信モジュールを含むことができる。ＵＥ８１８および／ま

たはＡＡＡ／ＲＰサーバ８２０は、各自のアプリケーションとＩＰ層通信モジュールとの間の通信を可能にするように構成することができる。ＯｐｅｎＩＤ識別プロバイダ（ＯＰ）は、例えばＭＮＯまたはＭＮＯに関連付けられたアプリケーションサービスプロバイダである。ＯＰサーバ８２１は複数のＭＮＯに対応することができ、広い顧客基盤がホットスポットを使用できるようにする。ＡＡＡサーバ８２０はＲＰとして実装することができ、ＵＥ８１８および／またはＯＰサーバ８２１上の鍵８２２（例えばアプリケーション層で導出される）を活用することができる。例示的実施形態によると、アプリケーション層の鍵８２２を活用してＥＡＰ－ＳＩＭ／ＡＫＡ認証を完了することができる。

【０１２１】

図８に示すように、８０１で、ＵＥ８１８はアクセスネットワークの通信（例えば、３ＧＰＰアクセスネットワーク通信）を介してＯＰサーバ８２１に対する認証を成功して完了することができる。８０１で、ＵＥ８１８とＯＰサーバ８２１は共有鍵８２２を設定することができる。共有鍵８２２は、例えばＵＥ８１８とＯＰサーバ８２１との間でアプリケーション層で確立されたアプリケーション層の認証情報である。ＵＥ８１８のローカルコンポーネント（例えば、接続マネジャ（ＣＭ））は、８０２で、例えば「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤなどのＡＰ８１９の識別の情報に基づいてＡＰ８１９を発見することができる。ＡＰ８１９の識別の情報は、例えばビーコンチャネルなどのアクセス層のシグナリングを介して発見することができる。ＵＥ８１８（例えば、ＣＭを実装している）は、サービスにアクセスするためにＡＰ８１９に切り替わるべきであると判断することができる。ＵＥ８１８は、ＡＰ８１９のネットワークの未許可クライアントである可能性がある。

【０１２２】

ＡＰ８１９（例えば認証者）は、８０３で、ＵＥ８１８の識別を求めるＥＡＰ要求を発行することができる。８０４で、ＵＥ８１８は、識別子、例えば自身の永続的な識別（例えば、移動加入者識別番号（ＩＭＳＩ））、仮名（pseudonym）識別、高速認証識別、またはＵＥ８１８の他の同様の識別子を返すことができる。アクセス層識別子は、例えば領域（realm）などの追加的な認証の情報と共に返すことができる。領域は、例えばシングルサインオン（ＳＳＯ）認証を使用するためのヒント（例えば、ＩＭＳＩ@ｓｓｏ．ＭＮＯ．ｃｏｍ）など、認証を行う際に使用する追加的な情報を含むことができる。

【０１２３】

ＡＰ８１９は、８０５でアクセス層識別子をＡＡＡ／ＲＰサーバ８２０に送信することができる。アクセス層識別子、およびＡＰ８１９とＡＡＡ／ＲＰサーバ８２０との間の他の通信は、例えばＲＡＤＩＵＳのアクセス要求、アクセスチャレンジ、および／またはアクセス受付けメッセージを使用して送信することができる。ＡＡＡ／ＲＰサーバ８２０は、ＡＡＡ／ＲＰサーバ８２０のアプリケーション層にアクセス層識別子を送信することができる。アクセス層識別子および／または事業者のポリシに基づいて、ＡＡＡサーバ８２０のＲＰ機能は、８０６でＯＰサーバ８２１の発見および／またはＯＰサーバ８２１との関連付けを行うことができる。発見および／または関連付けは、例えばＯｐｅｎＩＤプロトコルを使用して行うことができる。８０６の発見および／または関連付けの際に、ＡＡＡ／ＲＰサーバ８２０はアクセス層識別子をＯＰサーバ８２１に送信することができる。例えば、アクセス層識別子は、アプリケーション層でＡＡＡ／ＲＰサーバ８２０とＯＰサーバ８２１との間で送信することができる。ＯＰサーバ８２１は、アクセス層識別子および／またはアプリケーション層の認証情報８２２を使用して、ＡＡＡ／ＲＰサーバ８２０でＵＥ８１８の認証に使用することができる鍵材料を生成することができる。例えば、ＯＰサーバ８２１はアクセス層識別子を使用して、ＵＥ８１８に関連付けられたアプリケーション層の認証情報８２２を判定することができる。鍵材料は、アプリケーション層の認証情報８２２から鍵導出機能を使用して導出することができる。例示的実施形態によると、鍵材料は、ＵＥ８１８とＡＡＡ／ＲＰサーバ８２０との間の認証に使用できるセッション鍵を含むことができる。８０７で、ＯＰサーバ８２１は鍵材料をＡＡＡ／ＲＰサーバ８２０に送信することができる。

【０１２４】

ＡＡＡ／ＲＰサーバ８２０は、ＯＰサーバ８２１から受け取った鍵材料を使用して、ＥＡＰ－ＳＩＭ／ＡＫＡチャレンジをＵＥ８１８に送信することができる。ＥＡＰ－ＳＩＭ／ＡＫＡチャレンジを送信することにより、例えばＨＬＲ／ＨＳＳとインタフェースを取る、または通信する必要なく、再認証手順を可能にすることができる。８０８で、ＡＡＡ／ＲＰサーバ８２０は、アクセスチャレンジをＡＰ８１９に送信することができる。アクセスチャレンジは、ＵＥ８１８に関連付けられた識別子および／または８０７で受け取られた鍵材料を含むことができる。ＡＰ８１９は、８０９で、ＡＡＡ／ＲＰサーバ８２０から受信したＥＡＰメッセージ（例えば、ＥＡＰ－要求／チャレンジ）を無線アクセスネットワークを介してＵＥ８１８に送信することができる。ＥＡＰ－要求／チャレンジメッセージを受信すると、ＵＥ８１８は鍵材料を確認してメッセージの有効性を確認し、８１０でアプリケーション層の認証情報８２２を使用してＥＡＰレスポンスを生成することができる。例えば、ＵＥ８１８は、ＵＥ８１８に存在する高信頼環境（例えば、信頼できる処理モジュール、ＵＩＣＣ、ＳＩＭ、スマートカード等）にチャレンジを送信し、高信頼環境で鍵導出機能を使用してアプリケーション層の認証情報８２２から鍵材料を導出することができる。鍵材料は、アプリケーション層の認証情報を使用してＯＰサーバ８２１で生成された鍵材料と同じであってよい。例えば、鍵材料は、ＵＥ８１８とＡＡＡ／ＲＰサーバ８２０との間の認証に使用することが可能なセッション鍵を含むことができる。８１０で、鍵材料を使用してレスポンスを生成することができる。レスポンスは、ＵＥ８１８のアプリケーション層で生成し、ＡＰ８１９に送信するためにアクセス層に送ることができる。

【０１２５】

ＵＥ８１８は、８１１で、例えば再認証手順を使用して、ＥＡＰレスポンスメッセージの形態でＡＰ８１９にレスポンスを返すことができる。レスポンスは、ＵＥの識別子および／またはＵＥ８１８で生成された鍵材料（例えば、セッション鍵）を含むことができる。ＡＰ８１９は、８１２で、ＥＡＰ－レスポンス／チャレンジメッセージを、例えばアクセス要求メッセージの形態などでＡＡＡ／ＲＰサーバ８２０に転送することができる。８１２におけるアクセス要求は、ＥＡＰ　ＩＤおよび／または８１１でＵＥ８１８から得られた鍵材料を含むことができる。ＡＡＡ／ＲＰサーバ８２０は、８１２で、受信したメッセージの有効性を確認し、および／または受信したレスポンスが予想されるレスポンスと一致するかどうかを検査し、その検査が合格すると、ＡＡＡ／ＲＰサーバ８２０は、認証の成功および／またはＵＥ８１８がＷＬＡＮネットワークを使用してサービスにアクセスできることを知らせることができる。例えば、８１３で、ＡＡＡ／ＲＰ８２０は、アクセス受付けメッセージをＡＰ８１９に送信することができる。アクセス受付けメッセージは、ＥＡＰ成功の通知および／または鍵材料を含むことができる。ＡＰ８１９は、８１４でＥＡＰ成功の指示をＵＥ８１８に転送することができる。８１５で、ＡＰ８１９におけるＵＥ８１８のステータスが、ＡＰ８１９の使用を許可された状態になることができる。ＵＥ８１８に権限が付与されるのに伴って、ＵＥ８１８は、８１６でＤＨＣＰを使用してＩＰアドレスを取得することができる。例えば、ＵＥ８１８は、８１７で例えばそのＩＰアドレスを使用してＷＬＡＮネットワークを通じてインターネットにアクセスすることができる。

【０１２６】

図８に示す呼び出しフローまたはその一部を使用すると、ホットスポットのＡＡＡサーバ８２０は、ＥＡＰプロトコルを使用して認証を行うためにＭＮＯ　ＨＬＲ／ＨＳＳに接続せずに済む。例えば、本明細書に記載されるようにＯｐｅｎＩＤを使用することにより、例えばＡＡＡサーバ８２０または他のＲＰエンティティは、ユーザ認証を行うための例えばＨＬＲ／ＨＳＳまたは他のＳＳ７エンティティとの通信を回避することができる。代わりに、ＡＡＡサーバ８２０は、例えばＯｐｅｎＩＤ用のインターネットプロトコル（ＩＰ）に基づくＨＴＴＰ（Ｓ）インタフェースなどのＩＰに基づくＨＴＴＰ（Ｓ）インタフェースと通信することができる。

【０１２７】

図９は、ＲＰとして機能するＡＡＡサーバ９２３を使用する、ＥＡＰとＯｐｅｎＩＤとの統合を説明する別の流れ図である。図９に示すように、ＵＥ９２１および／またはそのユーザは、ＵＥ９２１、ＡＰ９２２、ＡＡＡ／ＲＰサーバ９２３、および／またはＯＰサーバ９２４間の通信を使用して、ＷＬＡＮ通信のための認証を受けることができる。ＵＥ９２１、ＡＡＡ／ＲＰサーバ９２３、および／またはＯＰサーバ９２４は各々、アプリケーション層の通信が可能なアプリケーションを含むことができる。ＵＥ９２１、ＡＰ９２２、および／またはＡＡＡ／ＲＰサーバ９２３は各々、ＩＰ層の通信が可能なＩＰ層通信モジュールを含むことができる。ＵＥ９２１および／またはＡＡＡ／ＲＰサーバ９２３は各々、各自のアプリケーションとＩＰ層通信モジュールとの間の通信を可能にするように構成することができる。例示的実施形態によると、ＡＰ９２２は、未許可のＵＥ９２１についてのＯｐｅｎＩＤの交換を可能にするように構成することができ、ＵＥ９２１は、ＡＰ９２２を介してＡＡＡ／ＲＰサーバ９２３および／またはＯＰサーバ９２４に到達し、通信することができる。

【０１２８】

図９に示す実施形態では、例えば図８に示すようにＵＥ９２１とＯＰサーバ９２４間で以前に共有されていた新しい鍵がない場合がある。したがって、ＵＥ９２１および／またはＯＰサーバ９２４は、認証およびアプリケーション層の識別鍵９２５の生成を行うことができる。ＡＡＡサーバ９２３はＲＰとして機能し、接続（例えば３ＧＰＰ接続）を使用してＯｐｅｎＩＤ認証を行うことができる。ＵＥ９２１は、複数のネットワークとの間に同時に接続を確立することが可能な装置とすることができる（例えばＵＥ９２１は、３ＧＰＰネットワークおよびＷＬＡＮホットスポットを同時に介して接続を確立することが可能なマルチＲＡＴ装置とすることができる）。図９に示すように、確立された３ＧＰＰ接続を使用してＯｐｅｎＩＤメッセージを交換し、ＥＡＰ－ＳＩＭ／ＡＫＡ認証を完了することができる。図９ではアクティブな３ＧＰＰ接続で確立された認証情報を使用してＷＬＡＮを通じた通信のための認証を行うが、他形態のワイヤレス接続を同様に使用して図９に示すように認証を行ってよいことは理解されよう。

【０１２９】

９０１で、ＵＥ９２１は、アクティブな３ＧＰＰ接続を確立し、その接続を通じてＡＡＡ／ＲＰサーバ９２３および／またはＯＰサーバ９２４に到達することができる。別の例示的実施形態によると、ＡＰ９２２は、９０１で確立された３ＧＰＰ接続を使用するのではなく、ＵＥ９２１の認証のためにＯｐｅｎＩＤの交換を可能にすることができる。いずれの実施形態でも、プロトコルの流れは図９に示すものと同じまたは同様である。引き続き図９のプロトコルフローを参照すると、ＵＥ９２１のローカルコンポーネント（例えばＣＭ）は、９０２でＡＰ９２２および／またはその識別情報、例えば「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤを発見することができる。ＡＰ９２２は、例えばビーコンチャネルなどのアクセス層のシグナリングを介して発見することができる。ＵＥ９２１のローカルコンポーネント（例えば、ＣＭ）は、ＵＥ９２１がＡＰ９２２に接続すべきであると判断することができる。ＵＥ９２１はＡＰ９２２においては未許可クライアントであり、ネットワークを通じたアクセスができない場合がある。

【０１３０】

９０３で、ＡＰ９２２（例えば、認証者）は、ＵＥ９２１のＩＰ層の識別を求めるＥＡＰ要求を発行することができる。ＵＥ９２１は、９０４でＥＡＰレスポンスを介して自身のＩＰ層識別を返すことができる。ＵＥ９２１のＩＰ層識別は、移動加入者識別番号（ＩＭＳＩ）および／または追加的な認証の情報を含むことができる。追加的な情報は例えばＵＥ９２１の領域を含むことができる。領域は、例えばＳＳＯ認証を使用するためのヒント（例えば、ＩＭＳＩ@ｓｓｏ．ＭＮＯ．ｃｏｍ）などの追加的な認証の情報を含むことができる。ＡＰ９２２は、９０５でＩＰ層の識別（ＥＡＰ　ＩＤ）をＡＡＡ／ＲＰサーバ９２３に送信することができる。ＩＰ層の識別ならびにＡＰ９２２とＡＡＡ／ＲＰサーバ９２３との間の他の通信は、ＲＡＤＩＵＳアクセスメッセージ、例えばＲＡＤＩＵＳアクセス要求メッセージ、ＲＡＤＩＵＳアクセスチャレンジメッセージ、および／またはＲＡ

ＤＩＵＳアクセス受付けメッセージなどを使用して送信することができる。
【０１３１】
ＡＡＡ／ＲＰサーバ９２３は、９０６でＯＰサーバ９２４を発見し、ＯＰサーバ９２４との関連付けを行うことができる。例えば、ＡＡＡサーバ９２３のＲＰ機能で、ＯｐｅｎＩＤプロトコルを使用してＯＰサーバ９２４の発見と関連付けを行うことができる。９０７で、ＵＥ９２１のアプリケーションが、リライングパーティ（ＲＰ）として機能することができるＡＡＡ／ＲＰサーバ９２４にログイン要求を送信することができる。９０７におけるログイン要求は、例えばＯｐｅｎＩＤを用いた３ＧＰＰ接続を通じて送信することができる。ＵＥ９２１のアプリケーションは、ＵＥ９２１のローカルエンティティ（例えば、ＣＭ）からの通信開始の指示に基づいてログイン要求を送信することができる。３ＧＰＰのワイヤレス接続を通じてＵＥ９２１と通信する間、ＡＡＡ／ＲＰサーバ９２３は、９０８でＵＥ９２１をＯＰサーバ９２４にリダイレクトすることができる。
【０１３２】
ＵＥ９２１は、９０９で３ＧＰＰ接続を通じてＯＰサーバ９２４に対して（ＯｐｅｎＩＤ認証情報を使用して）認証することができる。例えば、ＵＥは、ＯｐｅｎＩＤ認証情報を使用してＯＰに認証することができる。ＯＰサーバ９２４に対する認証が成功すると、アプリケーション層の認証情報９２５をＵＥ９２１および／またはＯＰサーバ９２４で確立することができる。ＯＰサーバ９２４は、アプリケーション層の認証情報９２５に基づいて鍵材料を生成することができる。鍵材料は、ＵＥ９２１とＡＡＡ／ＲＰサーバ９２３との間の認証に使用することができる。鍵材料は、鍵導出機能を使用してアプリケーション層の認証情報９２５から導出することができる。例示的実施形態によると、鍵材料は、ＡＡＡ／ＲＰサーバを使用した認証に使用されるセッション鍵を含むことができる。
【０１３３】
ＯＰサーバ９２４は、９１０で、アプリケーション層の認証情報９２５に基づく鍵材料をＡＡＡ／ＲＰサーバ９２３に送信することができる。ＡＡＡ／ＲＰサーバ９２３は、鍵材料をアプリケーション層で受信し、鍵材料をＡＰ９２２に送信するためにＩＰ層通信モジュールに通信することができる。ＡＡＡ／ＲＰサーバ９２３は、９１１で、鍵材料を使用してＡＰ９２２を介してＥＡＰ－ＳＩＭ／ＡＫＡチャレンジをＵＥ９２１に送信することができる。このチャレンジは再認証手順に基づくことができ、その場合ＡＡＡ／ＲＰサーバ９２３は例えばＨＬＲ／ＨＳＳと通信する必要なしに認証を行うことができる。９１１におけるチャレンジは、ＥＡＰ　ＩＤおよび／または９１０で受け取った鍵材料を含むことができる。ＡＰ９２２は９１１でチャレンジを受信し、９１２で、ＡＡＡ／ＲＰサーバ９２３から受信したＥＡＰメッセージ（ＥＡＰ－要求／チャレンジメッセージ）をＵＥ９２１に送信することができる。
【０１３４】
９１２でＥＡＰ－要求／チャレンジメッセージを受信すると、ＵＥ９２１は、９１３でアプリケーション層の認証情報９２５を使用してレスポンスを生成することができる。ＵＥ９２１は、ＡＡＡ／ＲＰサーバから受信した鍵材料を調べ、高信頼環境（例えば、信頼できる処理モジュール、ＵＩＣＣ、ＳＩＭ、スマートカード等）にチャレンジを送信し、高信頼環境はアプリケーション層の認証情報９２５を使用してレスポンスを生成する。例えば、ＵＥ９２１の高信頼環境は、鍵導出機能を使用してアプリケーション層の認証情報９２５から鍵材料を導出することができる。鍵材料は、ＯＰサーバ９２４でアプリケーション層の認証情報９２５を使用して生成された鍵材料と同じであってよい。例えば、鍵材料は、ＵＥ９２１とＡＡＡ／ＲＰサーバ９２３との間の認証に使用できるセッション鍵を含むことができる。９１３で、鍵材料を使用してレスポンスを生成することができる。レスポンスは、ＵＥ９２１のアプリケーション層で生成し、ＡＰ９２２に送信するためにアクセス層に送信することができる。
【０１３５】
ＵＥ９２１は、９１４で再認証手順に基づいてＥＡＰ－レスポンスメッセージでレスポンスをＡＰ９２２に返すことができる。ＥＡＰ－レスポンスメッセージは、ＩＰ層識別子

および／またはアプリケーション層の認証情報９２５から生成された鍵材料を含むことができる。ＡＰ９２２は、９１５でＥＡＰ－レスポンス／チャレンジメッセージをＡＡＡ／ＲＰサーバ９２３に転送することができる。ＡＡＡ／ＲＰサーバ９２３は、ＥＡＰ－レスポンス／チャレンジメッセージ内の鍵材料を検査することによりＵＥ９２１を認証することができ、検査が合格した場合、ＡＡＡ／ＲＰサーバ９２３は、ＵＥ９２１がＷＬＡＮネットワークを通じてサービスにアクセスすることを可能にすることができる。例えば、ＡＡＡ／ＲＰサーバ９２３は、ＥＡＰ成功および鍵材料を含むアクセス受付けメッセージを９１６でＡＰ９２２に送信することができる。９１７で、ＥＡＰ成功メッセージをＵＥ９２１に転送することができる。９１８で、ＵＥ９２１のステータスがＡＰ９２２で「許可」の状態になることができる。ＵＥ９２１は、９１９で例えばＤＨＣＰを使用してＡＰ９２２からＩＰアドレスを取得し、９２０でＷＬＡＮネットワークを通じてインターネットにアクセスすることができる。

【０１３６】

本発明ではＯｐｅｎＩＤを使用して、ＵＥ９２１とＯＰサーバ９２４との間で共有認証情報（例えばアプリケーション層の認証情報９２５）を作成する。アプリケーション層の認証情報９２５は、ＡＡＡ／ＲＰサーバ９２３でユーザ／ＵＥ９２１の認証に使用することができる。図９に示す実施形態は、ＵＥ９２１がＯＰサーバ９２４に対して認証し、秘密９２５を共有することを可能にする。ＵＥ９２１とＯＰサーバ９２４との間の認証により、ＵＥ９２１とＯＰサーバ９２４との間の（例えば、ＯｐｅｎＩＤ－ＡＫＡを使用した）認証が成功すると、アプリケーション層の認証情報９２５を生成できるようにする。次いで、ＯＰサーバ９２４は、アプリケーション層の認証情報９２５を使用してアサーションに署名し、アサーションは９１０でＡＡＡ／ＲＰサーバ９２３に送信され、次いでアプリケーション層の認証情報９２５を使用してＡＡＡ／ＲＰサーバ９２３によって検証される。例えばＯｐｅｎＩＤ手順の一部としてＯＰサーバ９２４とＵＥ９２１との間で秘密鍵９２５が生成されると、別のネットワークエンティティを使用してＥＡＰ認証情報（例えば、鍵材料）をＵＥ９２１に（例えば、ＵＥ９２１のＣＭに）送付することができる。

【０１３７】

この場合も、図９に示すプロトコルフローまたはその一部を使用すると、ホットスポットのＡＡＡサーバ９２３は、ＥＡＰプロトコルを使用して認証を行うためにＭＮＯ　ＨＬＲ／ＨＳＳに接続せずに済む。代わりに、ＡＡＡサーバ９２３は、例えばＯｐｅｎＩＤ用のインターネットプロトコル（ＩＰ）に基づくＨＴＴＰ（Ｓ）インタフェースなどの単純なＩＰに基づくＨＴＴＰ（Ｓ）インタフェースと通信することができる。ホットスポットのＡＰ９２２は、ＡＰメッセージまたは未許可状態の装置に加えてＯｐｅｎＩＤの交換を可能にすることができる。

【０１３８】

図１０は、ＲＰとして機能するＡＡＡサーバ１０２２を使用する、ＥＡＰとＯｐｅｎＩＤとの統合と、ローカルＯｐｅｎＩＤプロバイダ（ローカルＯＰ）の実装を説明する流れ図である。図１０に示すように、ＵＥ１０１８および／またはそのユーザは、ＵＥ１０１８、ＡＰ１０２１、ＡＡＡ／ＲＰサーバ１０２２、および／またはＯＰサーバ１０２３間の通信を使用して認証されることができる。図１０に示すように、ＵＥ１０１８は、ローカルＯＰ１０１９およびブラウジングエージェント（ＢＡ）／接続マネジャ（ＣＭ）１０２０を含むことができ、それぞれ相互および／または他のネットワークエンティティと通信して認証を行い、サービスへのアクセスを得るように構成される。図１０ではＢＡ／ＣＭ１０２０を１つのエンティティとして図示するが、ＢＡとＣＭは、ＵＥ１０１８内で独立した機能を行う別個のエンティティであってよい。ローカルＯＰ１０１９は、ＵＥ１０１８上のセキュアな環境（例えば、信頼できる処理モジュール、ＵＩＣＣ、ＳＩＭ、スマートカード等）内にインストールすることができる。ローカルＯＰ１０１９は、ＵＥ１０１８に対してＯＰサーバとして機能することができる。ローカルＯＰ１０１９は、ネットワーク上のＯＰサーバ１０２３と共有することができる長期間の秘密１０２４を含むことができる。ローカルＯＰ１０１９は、ローカルのユーザ認証が成功すると、識別のアサー

ションを作成および／または署名することができる。

【０１３９】

１００１で、ＵＥ１０１８はアクティブな３ＧＰＰ接続を有することができ、その接続を通じてＡＡＡ／ＲＰ１０２２および／またはＯＰサーバ１０２３に到達することができる（例えばＢＡ／ＣＭ１０２０を介して）。図１０では３ＧＰＰ接続とＷＬＡＮ接続間に認証とサービスの継続性を確立することができるが、他のネットワーク間の認証およびサービスの継続性のために同様の通信を使用できることは理解されよう。１００２で、ＢＡ／ＣＭ１０２０は、（例えば、アクセスネットワークで）ＡＰ１０２１および／またはその識別情報を発見することができる。この時点で、ＵＥ１０１８は、ＷＬＡＮネットワーク上では未許可クライアントである可能性がある。ＡＰ１０２１の識別の情報は、「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤを含むことができる。ＡＰ１０２３および／またはその識別の情報は、例えばビーコンチャネルなどのアクセス層のシグナリングを介して発見することができる。ＢＡ／ＣＭ１０２０は、ＵＥ１０１８がＡＰ１０２１に接続すべきであると判断することができる。１００３で、ＡＰ１０２１（例えば、認証者）は、ＵＥ１０１８の識別を求めるＥＡＰ要求を発行することができる。１００４で、ＵＥ１０１８は自身のＩＰ層識別を返すことができる。ＵＥ１０１８のＩＰ層識別は、移動加入者識別番号（ＩＭＳＩ）および／または機器の領域などの追加的な認証の情報を含むことができる。領域は、例えばＳＳＯ認証を使用するためのヒント（例えば、ＩＭＳＩ@ｓｓｏ．ＭＮＯ．ｃｏｍ）を含むことができる。

【０１４０】

１００５で、ＡＰ１０２１は、ＥＡＰ　ＩＤ（例えば、ＩＰ層識別）をＡＡＡ／ＲＰサーバ１０２２に送信することができる。１００６で、ＵＥ１０１８のＢＡ／ＣＭ１０２０は、ＨＴＴＰ　ＧＥＴ要求をＯｐｅｎＩＤ識別と共にＡＡＡ／ＲＰ１０２２に送信することができる。１００７で、ＡＡＡサーバ１０２２のＲＰ機能が、ＯＰサーバ１０２３の発見および／またはＯＰサーバ１０２３との関連付けを行うことができる。その結果、関連付け鍵１０２４および／または関連付けハンドルを作成し、ＯＰサーバ１０２３とＡＡＡ／ＲＰサーバ１０２２との間で共有することができる。例示的実施形態によると、ＯＰサーバ１０２３は、ＵＥ１０１８に関連付けられたアクセス層識別を受け取り、関連付け鍵１０２４および／または関連付けハンドルをアプリケーション層でＡＡＡ／ＲＰサーバ１０２２に送信することができる。ＡＡＡ／ＲＰサーバ１０２２は、その関連付け鍵１０２４からＥＡＰ鍵１０２５および／またはチャレンジを導出することができる。例えば、ＥＡＰ鍵１０２５は、鍵導出機能または逆ブートストラップ手順を使用して関連付け鍵１０２４から導出することができる。１００８で、ＡＡＡ／ＲＰサーバ１０２２は、認証のためにＵＥ１０１８をローカルＯＰ１０１９にリダイレクトすることができる。このＡＡＡ／ＲＰ１０２２からローカルＯＰ１０１９へのリダイレクトメッセージは関連付けハンドルを含むことができるが、関連付け鍵１０２４は含まなくてよい。

【０１４１】

１００９で、ＵＥ１０１８および／またはＢＡ／ＣＭ１０２０は、ローカルＯＰ１０１９に対してローカルに認証する、および／または署名されたアサーションを生成することができる。ＵＥ１０１８は、関連付けハンドルからローカルアサーション鍵１０２４を導出し、アサーション鍵１０２４を使用してアサーションに署名することができる。ローカルＯＰ１０１９へのリダイレクト要求は関連付けハンドルを含むことができ、ローカルＯＰ１０１９はその関連付けハンドルを使用して、ＯＰサーバ１０２３とＡＡＡ／ＲＰサーバ１０２２との間で共有されているものと同じ署名鍵１０２４を導出することができる。認証が成功して完了すると、署名済みのアサーションメッセージをローカルＯＰ１０１９で作成することができる。ローカルＯＰ１０１９は、１００７において生成されたＡＡＡ／ＲＰサーバ１０２２と同じＥＡＰ鍵１０２５も導出することができる。ステップ１００９の変形形態では、ＯｐｅｎＩＤプロトコルの実行を完了するために、１００９（ｂ）で、ローカルＯＰ１０１９が、検証のために署名済みアサーションメッセージと共にＢＡ／ＣＭ１０２０をＡＡＡ／ＲＰサーバ１０２２にリダイレクトすることができる。ローカル

ＯＰ１０１９とネットワークＯＰサーバ１０２３は、署名鍵１０２５の導出に使用できる長期間の秘密１０２４を共有することができる。

【０１４２】

ＡＡＡ／ＲＰサーバ１０２２は、生成されたＥＡＰ鍵１０２５に基づくＥＡＰチャレンジを生成することができる。ＥＡＰチャレンジはＥＡＰ－ＳＩＭ／ＡＫＡチャレンジとすることができ、ＨＬＲ／ＨＳＳと通信する必要なしにＵＥ１０１８に送信することができる。例えば、ＡＰ１０２１は、１０１０でＡＡＡ／ＲＰ１０２２からアクセスチャレンジを受信し、１０１１でＵＥ１０１８のＢＡ／ＣＭ１０２０にＥＡＰ要求を送信することができる。アクセスチャレンジおよびＥＡＰ要求は、ＥＡＰ識別および／またはＥＡＰチャレンジを含むことができる。ＥＡＰ－要求／チャレンジメッセージを受信すると、ＵＥ１０１８は、メッセージの有効性を確認し、および／またはＥＡＰ鍵１０２５を使用してレスポンスを生成することができる。例えば、ＵＥ１０１８は、ＵＥ１０１８上のセキュアな環境（例えば、信頼できる処理モジュール、ＵＩＣＣ、ＳＩＭ、スマートカード等）にチャレンジを送信し、セキュアな環境はＥＡＰ鍵１０２５を使用してＥＡＰレスポンスを生成することができる。

【０１４３】

ＵＥ１０１８は、１０１２でＡＰ１０２１にＥＡＰレスポンスを返すことができる。ＥＡＰレスポンスは、ＥＡＰ識別および／または共有鍵１０２５から生成されたＥＡＰ鍵１０２５を含むことができる。１０１３で、ＡＰ１０２１は、ＥＡＰ－レスポンス／チャレンジメッセージをＡＡＡ／ＲＰサーバ１０２２に転送することができる。ＡＡＡ／ＲＰサーバは、メッセージの有効性を確認し、導出されたＥＡＰ鍵１０２５に基づいて、受信したレスポンスを予想されるレスポンスと比較することができる。ＡＡＡ／ＲＰサーバ１０２２で行われる認証検査が合格すると、ＡＡＡ／ＲＰサーバ１０２２は１０１４で認証成功の通知をＡＰ１０２１に送信することができる。例えば、ＡＡＡ／ＲＰサーバ１０２２は、ＥＡＰ成功および鍵材料を含むアクセス受付けメッセージをＡＰ１０２１に送信することができる。認証成功の通知は１０１５でＵＥ１０１８に転送することができる。成功した認証が行われると、ＵＥ１０１８のステータスは、ＡＰ１０２１で通信を許可された状態になることができる。ＵＥ１０１８は、１０１６でＩＰアドレスを取得し（例えばＤＨＣＰを使用して）、１０１７でＡＰ１０２１を使用してＷＬＡＮを通じてインターネットにアクセスすることができる。

【０１４４】

図１０に示すプロトコルフローまたはその一部を使用すると、ホットスポットのＡＡＡサーバ１０２２は、ＥＡＰプロトコルを使用した認証を行うためにＭＮＯ　ＨＬＲ／ＨＳＳに接続せずに済む。また、ローカルＯＰ１０１９の使用により、ＵＥ１０１８がＥＡＰ処理のためのローカルな鍵の生成を行うことが可能となり、またローカルのユーザ認証も可能となる。

【０１４５】

図１１は、ＲＰとして機能するＡＡＡサーバ１１２１を使用するＥＡＰとＯｐｅｎＩＤとの統合を説明する別の流れ図である。ＡＡＡ／ＲＰ１１２１は、ＵＥ１０１８からのサービス要求の前に、既知のＯＰサーバとの関連付けの事前読み込みを開始することができる。図１１に示すように、ＵＥ１１１７および／またはそのユーザは、ＵＥ１１１７、ＡＰ１１２０、ＡＡＡ／ＲＰサーバ１１２１、および／またはＯＰサーバ１１２２間の通信を使用して、サービスへのアクセスのために認証を受けることができる。図１１に示す例示的実施形態によると、ＵＥ１１１７はローカルＯＰ１１１８を使用してローカル認証と、ＵＥ１１１７のＯｐｅｎＩＤ署名鍵１１２３からのＥＡＰ鍵１１２４の鍵生成を行うことができる。また、図１１に示す実施形態では、ＵＥ１１１７がＡＡＡ／ＲＰサーバ１１２１に対して認証する前に、ＯｐｅｎＩＤの識別子選択モードを使用してＡＡＡ／ＲＰサーバ１１２１とＯＰサーバ１１２２との間の関連付けを設定することができる。これにより、ＯＰサーバ１１２２とＡＡＡ／ＲＰサーバ１１２１との間の関連付けを事前に確立しておくことにより、ＯＰの発見を回避することが可能となる。その結果、例えばＵＥ１１

１７などのＵＥがアクセスネットワークに移動する際にＳＳＯ手順を完了するのに要する時間が短縮され、ネットワークのハンドオフをユーザに対してシームレスにすることが可能になる。

【０１４６】

例示的実施形態によると、ＡＡＡ／ＲＰサーバ１１２１は、例えばＯＰサーバ１１２２など、既知のＯＰサーバとの間に複数の関連付けを開始することができる。ＡＡＡ／ＲＰサーバ１１２１は、例えばＯｐｅｎＩＤの識別子選択モードを使用してそのような関連付けを開始することができる（その場合は、完全な識別子ＵＲＬの代わりにプロバイダのＵＲＬを使用することができ、プロバイダのＵＲＬは後にローカルＯＰ１１１８によって完全にすることができる）。ＡＡＡ／ＲＰサーバ１１２１は、ＯＰサーバから取得した関連付けハンドルおよび関連付けの秘密を記憶することができる。ＡＡＡ／ＲＰサーバ１１２１によって行われる発見および関連付けの１つは、１１０１におけるＯＰサーバ１１２１の発見と関連付けを含むことができる。ＡＡＡ／ＲＰ１１２１は、ＯＰサーバ１１２２から受け取った関連付けハンドルおよび／または関連付けの秘密１１２３を記憶することができる。

【０１４７】

１１０２で、ＵＥのローカルコンポーネント、例えばＢＡ／ＣＭ１１１９が、ＡＰの識別の情報に基づいてＡＰ１１２０を発見することができる。ＡＰ１１２０は、例えばアクセス層のシグナリングを介して特定することができる。この時点で、ＵＥ１１１７は、ＡＰ１１２０に関連付けられたネットワーク（例えば、ＷＬＡＮ）上では未許可クライアントである可能性がある。ＢＡ／ＣＭ１１１９は、ＵＥ１１１７がＡＰ１１２０に接続すべきであると判断することができる。１１０３で、ＡＰ１１２０は、ＵＥ１１１７のＩＰ層識別を要求することができる。ＵＥ１１１７は、１１０４で、自身のＩＰ層識別および／または追加的な認証の情報をＡＰ１１２０に返すことができる。ＡＰ１１２０は、１１０５でＵＥ１１１７のＩＰ層識別子をＡＡＡ／ＲＰサーバ１１２１に送信することができる。

【０１４８】

ＵＥ１１１７のＢＡ／ＣＭ１１１９は、１１０６でＯｐｅｎＩＤのプロバイダＵＲＬ、電子メールアドレス、または他のログイン識別子と共に（例えば、識別子選択モードで）ＡＡＡ／ＲＰ１１２１に要求を送信することができる。ＡＡＡ／ＲＰサーバ１１２１は、事前に設定された関連付けハンドルおよび関連付け鍵の１つを選択することができる。例えば、ＡＡＡ／ＲＰサーバ１１２１は、ＵＥ１１１７から受け取ったログイン識別子に基づいて、ＯＰサーバ１１２２との間で事前に設定された関連付けハンドルおよび関連付け鍵１１２３を選択することができる。ＡＡＡ／ＲＰサーバ１１２１は、その関連付け鍵１１２３からＥＡＰ鍵１１２４および／またはＥＡＰチャレンジを導出することができる。ＥＡＰ鍵１１２４は、例えば鍵導出機能または逆ブートストラップ手順を使用して関連付け鍵１１２３から導出することができる。ＡＡＡ／ＲＰ１１２１は、１１０７で、認証のためにＵＥ１１１７をローカルＯＰ１１１８にリダイレクトすることができる。ローカルＯＰ１１１８が配置されているので、認証をローカルＯＰ１１１８にリダイレクトすることができる。このローカルＯＰ１１１８へのリダイレクトは関連付けハンドルを含むことができるが、関連付けの秘密１１２３は含まなくてよい。

【０１４９】

ＵＥ１１１７および／またはＢＡ／ＣＭ１１１９は、１１０８でローカルＯＰ１１１８に対してローカルに認証することができる。ローカルＯＰ１１１８へのリダイレクト要求は関連付けハンドルを含むことができ、ローカルＯＰ１１１８はその関連付けハンドルを使用して、ＯＰサーバ１１２２とＡＡＡ／ＲＰ１１２１との間で共有される関連付け鍵１１２３を導出することができる。ローカルＯＰ１１１８およびネットワークＯＰサーバ１１２２は、署名鍵１１２３の導出に使用できる長期間の秘密を共有することができる。認証が成功して完了すると、ローカルＯＰ１１１８は、署名鍵１１２３からＥＡＰ鍵１１２４を導出することができ、ＥＡＰ鍵１１２４はＡＡＡ／ＲＰサーバ１１２１でも導出され

る。ＥＡＰ鍵は例えば鍵導出機能を使用して導出することができる。ローカルＯＰ１１１８はＥＡＰ鍵１１２４を使用して、ＡＡＡ／ＲＰサーバ１１２１に送信する署名済みアサーションメッセージを生成することができる。

【０１５０】

ＡＡＡ／ＲＰ１１２１は、生成したＥＡＰ鍵１１２４に基づくＥＡＰチャレンジを生成し、ＨＬＲ／ＨＳＳと通信する必要なしにそのＥＡＰチャレンジをＵＥ１１１７に送信することができる。例えば、アクセスチャレンジは１１０９でＡＡＡ／ＲＰ１１２１からＡＰ１１２０に送信することができる。アクセスチャレンジはＥＡＰ　ＩＤおよび／またはチャレンジを含むことができる。１１１０で、ＡＰ１１２０は、ＡＡＡ／ＲＰサーバ１１２１から受信したＥＡＰメッセージ（ＥＡＰ－要求／チャレンジ）をＢＡ／ＣＭ１１１９に送信することができる。

【０１５１】

ＥＡＰ－要求／チャレンジメッセージを受信すると、ＵＥ１１１８はメッセージの有効性を確認し、ＥＡＰ鍵１１２４を使用してレスポンスを生成することができる。ＵＥ１１１８はＥＡＰチャレンジを高信頼環境（例えば、信頼できる処理モジュール、ＵＩＣＣ、ＳＩＭ、スマートカード等）に送信し、高信頼環境はＥＡＰ鍵１１２４を使用してＥＡＰレスポンスを生成することができる。ＵＥ１１１７は、１１１１でレスポンスメッセージをＡＰ１１２０に返すことができる。レスポンスメッセージは、ＥＡＰ　ＩＤおよび／またはＥＡＰレスポンスを含むことができる。１１１２で、ＡＰ１１２０はＥＡＰ－レスポンス／チャレンジメッセージをＡＡＡ／ＲＰサーバ１１２１に転送する。ＡＡＡ／ＲＰはＥＡＰ鍵１１２４を使用して認証を行うことができる。ＡＡＡ／ＲＰサーバ１１２１で行われる認証検査が合格すると、ＡＡＡ／ＲＰサーバ１１２１は、１１１３で認証成功の通知を送信することができる。例えば、ＡＡＡ／ＲＰサーバ１１２１は、認証の成功を知らせるメッセージをＡＰ１１２０に送信することができる。例えば、認証成功の通知は、ＥＡＰ成功および鍵材料を含むことができる。認証成功の通知は、１１１４でＵＥ１１１７に転送することができる。成功した認証が行われると、ＵＥ１１１７のステータスはＡＰ１１２０上で「許可」の状態になることができる。ＵＥ１１１７は、１１１５でＡＰ１１２０で通信するためのＩＰアドレスを（例えば、ＤＨＣＰを使用して）取得し、１１１６でＡＰ１１２０を使用してインターネットにアクセスすることができる。

【０１５２】

図１２は、ＡＡＡサーバ１２１８をＯＰサーバとして実装する認証プロトコルを説明する流れ図である。図１２に示す流れ図は、ＵＥ１２１６、ＡＰ１２１７、およびＡＡＡ／ＯＰサーバ１２１８を使用して実施することができる。ＡＰ１２１７は、ホットスポット、または例えばＷＬＡＮネットワークを通じて通信可能な他のノードとすることができる。ホットスポットのＡＡＡサービスにＯＰサーバの機能を組み込むことにより、例えば３ＧＰＰネットワークとＷＬＡＮネットワークとの間など、ネットワーク間のシームレスな認証および／またはサービスの継続性の支援を可能にすることができる。ＡＡＡ／ＯＰサーバ１２１８は、ＵＥ１２１６および／またはＡＡＡ／ＯＰサーバ１２１８上の事前に生成された鍵１２１９を使用して、ＷＬＡＮネットワークを通じてサービスにアクセスするための認証を行うことができる。例示的実施形態によると、事前に生成された鍵１２１９はアプリケーション層の認証情報である。図１２では３ＧＰＰネットワークとＷＬＡＮネットワークとの間のシームレスな認証および／またはサービスの継続性のためのネットワーク通信を説明するが、同様の通信を他の種類のワイヤレスネットワーク間のシームレスな認証およびサービスの継続性に使用できることは理解されよう。

【０１５３】

本明細書に記載されるように、ユーザは、公衆のホットスポット（例えば、ＡＰ１２１７）で、ＡＡＡサーバ１２１８に組み込まれたＯＰモジュールに対してシームレスに認証されることができる。一実施形態によると、ＡＡＡ／ＯＰサーバ１２１８を使用して認証を行って、ＵＥ１２１６および／またはＡＡＡ／ＯＰサーバ１２１８で導出された鍵１２１９を活用して認証（例えば、ＥＡＰ－ＳＩＭ／ＡＫＡ認証）を完了することができる。

アクティブな３ＧＰＰ接続を使用して、ＷＬＡＮネットワークで認証するための認証メッセージ（例えば、ＯｐｅｎＩＤ認証メッセージ）を交換することができる。

【０１５４】

図１２に示すように、ＵＥ１２１６は、１２０１で、３ＧＰＰアクセスネットワークを通じてＡＡＡ／ＯＰサーバ１２１８に対する認証を成功させて完了することができる。３ＧＰＰアクセスネットワークを通じた認証プロトコル時に、共有鍵１２１９をＵＥ１２１６および／またはＡＡＡ／ＯＰサーバ１２１８で確立することができる。１２０２で、ＵＥのローカルコンポーネント（例えば、ＣＭ）がＡＰの識別の情報に基づいてＡＰ１２１７を発見することができる。ＡＰ１２１７の識別の情報は例えば「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤである。ＡＰ１２１７は、例えばビーコンチャネルなどのアクセス層のシグナリングを介して発見することができる。ＵＥ１２１６のローカルコンポーネント（例えば、ＣＭ）は、ＵＥ１２１６がそのホットスポットに切り替わるべきであると判断することができる。

【０１５５】

ＡＰ１２１７（例えば、認証者）は、１２０３で、ＵＥ１２１６のＩＰ層識別を求めるＥＡＰ要求を発行することができる。ＵＥ１２１６は、１２０４で自身のＩＰ層識別および／または追加的な認証の情報をＡＰ１２１７に返すことができる。例えば、ＵＥ１２１６は自身の移動加入者識別番号（ＩＭＳＩ）を返すことができる。追加的な認証の情報は領域を含むことができる。領域は、ＳＳＯ認証を使用するためのヒント（例えば、ＩＭＳＩ@ｓｓｏ．ＭＮＯ．ｃｏｍ）を含む。例示的実施形態によると、ＵＥ１２１６は、ＩＭＳＩの先頭にビット（「０」または「１」）を付加して、それぞれＥＡＰ－ＡＫＡ手順を使用するのか、またはＥＡＰ－ＳＩＭ手順を使用するのかをサーバに示唆すること等により、ＵＥ１２１６の認証能力の発見を支援する追加的情報を提供することができる。

【０１５６】

ＡＰ１２１７は、１２０５で、ＥＡＰ　ＩＤ（例えば、アクセス層識別）をＡＡＡ／ＯＰサーバ１２１８に送信することができる。ＡＡＡサーバ１２１８のＯＰ機能が、１２０６で、ＵＥ１２１６と共有される、事前に生成された鍵１２１９に基づいてチャレンジを生成することができる。例えば、ＡＡＡ／ＯＰサーバ１２１８は、アクセス層の認証で使用するセッション鍵を導出することができる。セッション鍵は、例えば鍵導出機能または汎用的なブートストラップ手順を使用して導出することができる。ＡＡＡ／ＯＰサーバ１２１８は再認証手順を使用して、ＥＡＰ－ＳＩＭ／ＡＫＡチャレンジメッセージでＵＥ１２１６にチャレンジを送信することができる。例えば、ＡＰ１２１７は、１２０７で、共有鍵１２１９から生成されたセッション鍵および／またはＡＡＡ／ＯＰサーバ１２１８からのＥＡＰ　ＩＤを含むＥＡＰメッセージを受信することができる。次いで、ＡＰ１２１７は、ＡＡＡ／ＯＰサーバから受信したＥＡＰメッセージ（ＥＡＰ－要求／チャレンジ）を１２０８でＵＥ１２１６に転送することができる。

【０１５７】

ＥＡＰ－要求／チャレンジメッセージを受信すると、ＵＥ１２１６はセッション鍵を使用して認証を行うことができる。ＵＥ１２１６は、ＵＥ１２１６に常駐するセキュアな環境（例えば、信頼できる処理モジュール、ＵＩＣＣ、ＳＩＭ、スマートカード等）にチャレンジを送り、セキュアな環境は１２０９でＡＡＡ／ＯＰサーバ１２１８との共有鍵１２１９を使用してＥＡＰレスポンスを生成することができる。例えば、ＥＡＰレスポンスメッセージは、共有鍵１２１９から生成されたレスポンスを含むことができる。

【０１５８】

ＵＥ１２１６は、１２１０で、再認証手順に基づいて、ＡＰ１２１７へのレスポンスでＥＡＰメッセージをＡＰ１２１７に返すことができる。ＥＡＰメッセージは、ＥＡＰ　ＩＤおよび／または共有鍵１２１９を使用して生成されたレスポンスを含むことができる。１２１１で、ＡＰ１２１７は、ＥＡＰ－レスポンス／チャレンジメッセージをＡＡＡ／ＯＰサーバ１２１８に転送することができる。ＡＡＡ／ＯＰサーバは、メッセージの有効性を確認し、および／またはＥＡＰ－レスポンス／チャレンジメッセージで受信したレスポ

ンスを予想されるレスポンスと比較することができる。ＡＡＡ／ＯＰサーバ１２１８で行われる検査に合格すると、ＡＡＡ／ＯＰサーバ１２１８は、ＡＰ１２１７を介して認証成功の通知をＵＥ１２１６に送信することができる。例えば、ＡＡＡ／ＯＰサーバ１２１８は、１２１２でＥＡＰの成功および／または鍵材料を含むアクセス受付けメッセージをＡＰ１２１７に送信することができる。ＥＡＰ成功メッセージは１２１３でＵＥ１２１６に転送することができる。認証が成功すると、ＵＥ１２１６のステータスがＡＰ１２１７で「許可」の状態になることができる。ＵＥ１２１６は、１２１４でＡＰ１２１７からＩＰアドレスを（例えばＤＨＣＰを使用して）取得し、１２１５でＷＬＡＮネットワークを通じてインターネットにアクセスすることができる。

【０１５９】

本明細書に記載されるように、ＵＥ１２１６とＡＡＡ／ＯＰサーバ１２１８との間で共有認証情報１２１９を生成することができる。共有認証情報は、例えば別のネットワークにおける認証中または認証後に確立することができる。ＵＥ１２１６は、ＡＡＡ／ＯＰサーバ１２１８に対して認証することができ、ＡＡＡ／ＯＰサーバ１２１８は共有認証情報１２１９を使用してアサーションに署名し、アサーションはＲＰに送信され、次いで共有認証情報１２１９を使用してＲＰによって検証される。認証（例えば、ＯｐｅｎＩＤ－ＡＫＡを使用する）が成功すると、ＵＥ１２１６とＡＡＡ／ＯＰ１２１８との間の認証で共有認証情報１２１９を生成することができる。ＡＡＡ／ＯＰ１２１８とＵＥ１２１６との間で共有認証情報１２１９が生成されると、別のエンティティがＥＡＰの認証情報をＵＥ１２１６に（例えば、ＣＭに）送付することができる。

【０１６０】

本明細書に記載の実施形態は、複雑なＭＡＰ／ＤｉａｍｅｔｅｒインタフェースをホットスポットのＡＡＡサーバで実装する必要、またはＡＶフェッチングのためにＭＮＯ　ＨＬＲ／ＨＳＳとインタフェースを取り、通信する必要をなくすことができる。また、３ＧＰＰとＷＬＡＮホットスポットとの間のシームレスな認証およびサービスの継続性を可能にすることができる。図１２に示すように、ホットスポットのＡＡＡサーバ１２１８にＯＰモジュールを実装することができる。ホットスポットのＡＡＡサーバにＯＰを組み込む代替として、またはそれに加えて、ＭＮＯ　ＡＡＡサーバにＯＰ機能を実装し、ホットスポットのＡＡＡサーバがＡＡＡプロキシとして機能し、要求をＭＮＯ　ＡＡＡサーバに中継することもできる。

【０１６１】

図１３は、ＯｐｅｎＩＤメッセージをＥＡＰプロトコルメッセージに組み込むためのプロトコルフローの例示的実施形態を示す。このプロトコルフローまたはそれに同様のプロトコルフローを実装して、例えば図１１および図１２に示すネットワーク通信の一部を可能にすることができる。

【０１６２】

図１３に示すように、ＵＥ１３１６、ＡＰ／ＲＰ１３１７、および／またはＯＰサーバ１３１８が通信を行って、ネットワークにおけるＵＥ１３１６の認証を可能にすることができる。ＵＥ１３１６は、１３０１でＡＰ／ＲＰ１３１７に関連付けられたアクセスネットワークを発見することができる。この時点で、ＵＥ１３１６は、ネットワーク上の通信を許可されていない可能性がある。１３０２で、ＡＰ／ＲＰ１３１７は、ＥＡＰ　ＩＤ（例えば、アクセス層識別）の要求を送信することができる。ＵＥ１３１６は、１３０３で、ＡＰ１３１７へのＥＡＰレスポンスでＯｐｅｎＩＤ識別子を送信することができる。ＯｐｅｎＩＤ識別子を使用して、１３０４で、ＡＰ１３１７は、ＯＰサーバ１３１８の発見および／またはＯＰサーバ１３１８とのＯｐｅｎＩＤプロトコルの関連付けのステップを行うことができる。発見および／または関連付けを行うために、ＡＰ１３１７は、ＯｐｅｎＩＤメッセージ（例えば、ＯｐｅｎＩＤ識別子）をＥＡＰプロトコルからアンラップ（unwrap）し、ＨＴＴＰ（Ｓ）を介してＯＰサーバ１３１８と通信することができる。ＯｐｅｎＩＤプロトコルでの関連付けの確立は任意であってよい。

【０１６３】

関連付け後、ＯＰサーバ１３１８は１３０５でチャレンジを生成し、ＡＰ１３１７は１３０６でＯＰサーバ１３１８からＯｐｅｎＩＤチャレンジを受信することができる。ＡＰ１３１７は、１３０７でＥＡＰ要求（ＯｐｅｎＩＤプロトコルのＯｐｅｎＩＤリダイレクトに対応する）をＵＥ１３１６に送信することができる。ローカルＯＰの助けを借りて、ＵＥ１３１６は、１３０８で適切なレスポンスを生成し、１３０９でＥＡＰレスポンスを署名済みのＯｐｅｎＩＤアサーションと共にＡＰ１３１７に送信することができる。ＡＰ１３１７がＯＰサーバ１３１８との関連付けを確立している場合は、ＡＰ１３１７は、アサーション署名を自律的に検証し、したがってＵＥ１３１６を認証し、権限を付与することができる。事前に関連付けが確立されていない場合は、ＡＰ１３１７は、例えば１３１０で、ステートレスモードを使用してＯＰサーバ１３１８による署名の検証を要求することができる。ＯＰサーバ１３１８で認証が成功した場合、ＯＰサーバ１３１８は、１３１１でＯｐｅｎＩＤメッセージを識別および認証アサーションと共にＡＰ／ＲＰ１３１７に送信することができる。ＡＰ／ＲＰ１３１７は、１３１２でＵＥ１３１６に認証の成功を通知し、１３１３でＵＥはＡＰ／ＲＰ１３１７を介してサービスを許可されることができる。１３１４で、ＵＥ１３１６はＡＰ／ＲＰ１３１７からＩＰアドレスを取得し（例えば、ＤＨＣＰ要求を介して）、１３１５でＷＬＡＮネットワークを通じたインターネットアクセスを許される。

【０１６４】

ステートレスモードは、ＡＰ１３１７とＯＰサーバ１３１８とがすでに関連付けを確立している場合でも、ローカルＯＰによって「強制」することができる。ローカルＯＰは、アサーションメッセージ中に「ｉｎｖａｌｉｄａｔｅ＿ｈａｎｄｌｅ」のフィールドを設定し、新しい関連付けハンドルを作成することができる。次いで、ＡＰ１３１７は、署名の検証のためにＯＰサーバ１３１８に戻ることができる。ローカルＯＰが配置され、アサーションを発行する場合でも、ＯｐｅｎＩＤの動作を使用してＡＰ１３１７からＯＰサーバ１３１８へのフィードバック機構をトリガすることができる。関連付けが使用されており、無効にされない場合は、ＯＰサーバ１３１８へのフィードバックはなくてよい。本明細書に記載の実施形態は、例えば何らかの支払いシナリオおよび／またはプライバシーを可能にすることができる。

【０１６５】

例示的実施形態によると、サービスのためのユーザ認証は、ＥＡＰプロトコルのＡＶフェッチングのためにＡＰとＭＮＯのＡＡＡサーバとの間に接続を確立することによって行うことができる。ＯｐｅｎＩＤを実装することにより、ＡＰとＭＮＯネットワークとの間に追加的な抽象化層を作り出すことができる。ＯＰは、ネットワークの認証基盤に対してプロキシとして機能し、ＡＰに接続されたネットワークＡＶへの直接のアクセスを与えることなく、ネットワーク認証情報に基づいてＵＥを認証することができる。ＯＰが認証点として機能するので、ＡＰのロジックを減らしてＯｐｅｎＩＤのアサーションを検証することができる。ＯｐｅｎＩＤを使用すると、ＡＰでＡＶを扱う必要がなくなる。また、ＡＰがＭＮＯの基盤への直接の接続を有する必要がないため、ＯＰが、異なるＡＰ事業者の複数のＡＰに対応することができる。ＯＰは、トランザクションの認証者としても機能することができる（これは、例えばローカルＯＰを含むことができる）。これにより、ＡＰ事業者に対してはＭＮＯのバックエンドを介した課金および／または利益／特典の支払いを可能にすることができる。したがって、複数のＭＮＯが同じＯＰを使用することができる。複数のＡＰ提供者も同じＯＰを使用することができる。その結果、例えば「スター型」のアーキテクチャとなる。

【０１６６】

本明細書に記載の実施形態では、汎用的なブートストラップ手順などの鍵導出機能を使用することができる。例えば、汎用ブートストラッピングアーキテクチャ（ＧＢＡ）を実装することができる。ＧＢＡの例示的実施形態の１つが、３ＧＰＰ技術仕様（ＴＳ）３３．２２０に記載される。ただし、ＧＢＡはＵＩＣＣによる認証情報に制限される場合がある。本明細書に記載の実施形態は、ＵＩＣＣによる認証情報および／または非ＵＩＣＣの

認証情報を使用して実装することができる。ＧＢＡは、ブートストラップおよび認証を行うためのＵＥ－ＢＳＦとＵＥ－ＮＡＦ間のＩＰ接続にも制限される場合がある。その結果、ＧＢＡでは、例えばＭｏｂｉｌｅ　ＩＰなどのシームレスな移動性プロトコルを中断させる可能性がある。Ｍｏｂｉｌｅ　ＩＰでは、ＩＰ層またはそれより下位層での認証を使用して、切替えと、ＷＬＡＮインタフェースなどの新しいインタフェースの立ち上げおよびホームエージェント（ＨＡ）への登録を行うことができる。ＩＰ層におけるＭｏｂｉｌｅ　ＩＰ登録とアプリケーション層におけるＧＢＡによるブートストラップとの間の競合状態は、移動性を破綻させ、ＭＩＰ登録を失敗させ、その結果ＷＬＡＮネットワークへの切替えが失敗する可能性がある。

【０１６７】

ＥＡＰとＧＢＡの統合の選択肢を使用して、例えばＧＢＡに基づくデュアルモード装置の場合の３ＧＰＰとＷＬＡＮネットワークとの間の移動性の問題を解決することができる。ＧＢＡ認証は、既存の３ＧＰＰインタフェースを通じて行うことができる。ＧＢＡ認証の結果（例えば装置に記憶されたＫｓ＿ＮＡＦ）を使用して、ホットスポットでＥＡＰ認証を完了することができる。移動性の問題は、例えば、３ＧＰＰインタフェースを介してＧＢＡ認証のためのＩＰ接続性を提供すること、およびＧＢＡとＥＡＰの統合を使用することによってＧＢＡで解決することができる。

【０１６８】

図１４は、ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔを使用したサービスのためのＵＥ１４２１の認証を説明する流れ図である。図１４に示すように、ＵＥ１４２１は、アクティブなワイヤレス接続（例えば、３ＧＰＰ接続）を有することができ、その接続を通じてＡＡＡ／ＲＰサーバ１４２５および／またはＯＰサーバ１４２６に到達することができる。１４０１で、ＵＥ１４２１は、ＡＡＡ／ＲＰサーバ１４２５にＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔログインを行い、ＡＡＡ／ＲＰサーバ１４２５はアクセストークンを作成することができる。アクセストークンは１４０２でＢＡ１４２２によって保存（またはＯＳによって保存）されることができる。ＵＥのローカルコンポーネント、例えばＣＭ１４２３が、ビーコンチャネル等のアクセス層のシグナリングを介してＡＰ１４２４および「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤなどのその識別の情報を発見することができる。ＣＭ１４２３は、ＵＥ１４２１がＡＰ１４２４に接続すべきであると判断することができる。１４０３で、ＣＭはＡＰ１４２４にアタッチすることができる。ＡＰ１４２４（例えば、認証者）は、１４０４でＵＥ１４２１の状態を「未認証」または「未許可」に設定することができる。

【０１６９】

１４０５で、ＡＰ１４２４は、ＵＥ１４２１のＥＡＰ／ＩＰ層の識別を求めるＥＡＰ要求を発行することができる。１４０６で、ＵＥ１４２１は、移動加入者識別番号（ＩＭＳＩ）および／または他の認証の情報を返すことができる。他の認証の情報は領域を含むことができ、領域は、例えばＳＳＯ認証を使用するためのヒント（例えば、ＩＭＳＩ@ｓｓｏ．ＭＮＯ．ｃｏｍ）を含むことができる。１４０７で、ＡＰ１４２４は、ＵＥ１４２１から受け取ったＥＡＰ　ＩＤをＡＡＡ／ＲＰサーバ１４２５に（例えば、ＲＡＤＩＵＳアクセス要求を使用して）送信することができる。

【０１７０】

１４０８で、ＡＡＡ／ＲＰサーバ１４２５は、受け取ったＥＡＰ　ＩＤに基づいて（または受け取ったＥＡＰ　ＩＤを使用してデータベースを検索することにより）、ＵＥ１４２１がＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔに基づくフローを使用できることを検出することができる。ＡＡＡ／ＲＰサーバ１４２５は、１４０９でＡＰ１４２４にＥＡＰ－ＳＩＭ／ＡＫＡチャレンジを送信し、ＯｐｅｎＩＤ　ＣｏｎｎｅｃｔをＥＡＰプロトコルで使用すべきことを知らせることができる。ＡＰ１４２４は、ＡＡＡ／ＲＰサーバ１４２５から受信したＥＡＰメッセージ（ＥＡＰ－要求／チャレンジ）をＵＥ１４２１に（例えば、ＣＭ１４２３に）送信することができる。

【０１７１】

ＥＡＰ－要求／チャレンジメッセージを受信すると、１４１１で、ＵＥ１４２１はメッ

セージ中の認証パラメータを調べ、ＢＡ１４２２にトークンを要求することができる（例えばＢＡは代わりにＯＳまたはＡＰＩであってもよい）。１４１２でアクセストークンをＣＭ１４２３に返すことができる。１４１３で、ＣＭ１４２３は、アクセストークンをＥＡＰメッセージでＡＰ１４２４に送信することができる。ＡＰ１４２４は、１４１４で、ＥＡＰレスポンス／チャレンジメッセージをＡＡＡ／ＲＰサーバに転送することができる。ＡＡＡ／ＲＰサーバ１４２５は、１４１５で、トークンを検証し、ＯＰサーバ１４２６からのユーザ情報エンドポイントと共にトークンを使用して、ＯＰサーバ１４２６から認証用のユーザ情報を取り出すことができる。

【０１７２】

ＯＰサーバ１４２６は、ユーザ情報を公開する前にトークンの有効性を確認することができる。ＡＡＡ／ＲＰサーバ１４２５は、１４１７でユーザ情報を受け取ることができる。ユーザ情報は、例えばユーザ名、住所、課金情報、および／または課金トークンを含むことができる。ＡＡＡ／ＲＰサーバ１４２５は、１４１７で、受信したユーザ情報に基づいて認証の検査を行うことができる。すべての検査が合格すると、ＡＡＡ／ＲＰサーバは、認証成功の通知をＵＥ１４２１に送信することができる。例えば、ＡＡＡ／ＲＰサーバ１４２５は、１４１８で、ＥＡＰ成功および鍵材料を含むアクセス受付けメッセージをＡＰ１４２４に送信することができる。ＥＡＰ成功メッセージは、１４１９でＵＥ１４２１に転送することができる。１４２０で、ＵＥ１４２１のステータスが、ＡＰ１４２４でネットワーク上でアクセスを許可された状態になる。ＵＥ１４２１は、ＩＰアドレスを取得し（例えばＤＨＣＰを使用して）、ＡＰ１４２４を介してインターネットにアクセスすることができる。

【０１７３】

図１５は、ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔおよびローカルを使用した、サービスのためのＵＥ１５２０の認証を説明する流れ図である。図１５に示すように、ＵＥ１５２０のローカルコンポーネント、例えばＣＭ１５２２がＡＰ１５２４、および／またはその識別の情報を発見することができる。ＡＰ１５２４および／またはその識別の情報は「ＭＮＯ－ＷｉＦｉ」ＳＳＩＤを含むことができ、例えばビーコンチャネルなどのアクセス層のシグナリングを介して発見することができる。ＣＭ１５２２は、ＵＥ１５２０がＡＰ１５２４に接続すべきであると判断することができる。

【０１７４】

１５０１で、ＵＥ１５２０はＡＰ１５２４にアタッチすることができる。ＡＰ１５２４（例えば、認証者）は、１５２０でＵＥ１５２０の状態を通信について未認証または未許可の状態に設定することができる。ＡＰ１５２４は、１５０３でＵＥのＩＰ層／ＥＡＰ識別を求めるＥＡＰ要求を発行することができる。ＵＥ１５２０は、１５０４で自身のＩＰ層／ＥＡＰ識別子を返すことができる。例えば、ＵＥ１５２０は、移動加入者識別番号（ＩＭＳＩ）および／または追加的な認証の情報を返すことができる。追加的な認証の情報はＵＥの領域を含むことができ、領域は、例えばＳＳＯ認証を使用するためのヒント（例えば、ＩＭＳＩ@ｓｓｏ．ＭＮＯ．ｃｏｍ）を含むことができる。

【０１７５】

ＡＰ１５２４は、１５０５でＥＡＰ　ＩＤをＡＡＡ／ＲＰサーバ１５２５に送信することができる。ＡＰ１５２４とＡＡＡ／ＲＰサーバ１５２５との間の通信は、例えばアクセス要求メッセージ、アクセスチャレンジ、および／またはアクセス受付けメッセージなどのＲＡＤＩＵＳメッセージを使用して行うことができる。１５０６で、ＡＡＡ／ＲＰサーバは、受け取ったＥＡＰ識別に基づいて、ＵＥ１５２０がＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔに基づくフローを使用できることを検出することができる（または例えば受け取ったＥＡＰ識別を使用してデータベースを検索することにより）。ＡＡＡ／ＲＰサーバは、１５０７でＥＡＰ－ＳＩＭ／ＡＫＡチャレンジをＡＰ１５２４に送信することができる。このチャレンジは、ＯｐｅｎＩＤ　ＣｏｎｎｅｃｔをＥＡＰプロトコルで使用することを指示することができる。指示は、ＡＰ１５２４および／またはＥＡＰプロトコルに対して透過にすることができる。指示に代えて、ＡＡＡ／ＲＰサーバ１５２５は、ＯｐｅｎＩＤ　Ｃｏ

ｎｎｅｃｔ要求オブジェクト（例えば、ＪＳＯＮ）を作成し、要求中に指示子（ＵＲＬ）を入れてもよい。

【０１７６】

１５０８で、ＡＰ１５２４は、ＡＡＡ／ＲＰサーバ１５２５から受信したＥＡＰメッセージ（ＥＡＰ－要求／チャレンジ）をＵＥ１５２０に（例えば、ＣＭ１５２２に）送信することができる。ＥＡＰ－要求／チャレンジメッセージを受信すると、１５０９で、ＵＥ１５２０は認証パラメータを調べることができ、ＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ要求オブジェクトを使用して、ローカルＯＰ１５２１とのＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔセッションを開始する。ローカルＯＰ１５２１は、１５１０でアクセストークンを作成することができる（例えばローカルのユーザ認証が成功した後に）。１５１１で、アクセストークンをＣＭ１５２２に返すことができる。１５１２で、ＣＭ１５２２は、アクセストークンをＥＡＰメッセージでＡＰ１５２４に送信することができる。ＡＰ１５２４は、ＥＡＰ－レスポンス／チャレンジメッセージをＡＡＡ／ＲＰサーバ１５２５に転送することができる。ＡＡＡ／ＲＰサーバ１５２５は、１５１４でトークンを検証し、トークンをＯＰサーバ１５２６からのユーザ情報エンドポイントと共に使用して、認証用のユーザデータを取り出すことができる。

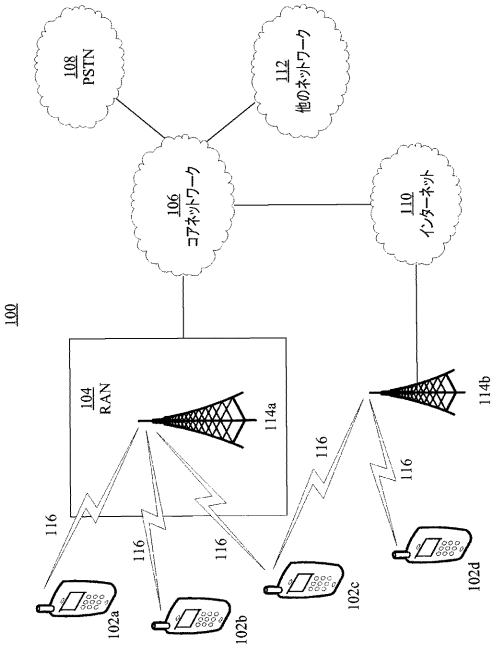
【０１７７】

１５１５で、ＯＰサーバ１５２６は、トークンの有効性を確認してから認証用のユーザ情報を公開することができる。ＡＡＡ／ＲＰサーバ１５２５は、１５１６でユーザ情報を受信することができる。ユーザ情報は、例えばユーザ名、住所、課金情報、および／または課金トークンを含むことができる。ＡＡＡ／ＲＰサーバ１５２５は、１５１６で受け取ったユーザ情報を使用してユーザの認証を行い、検査が合格であると、ＡＡＡ／ＲＰサーバ１５２５は１５１７で認証成功の通知をＵＥ１５２０に送信することができる。例えば、ＡＡＡ／ＲＰサーバ１５２５は、ＥＡＰ成功メッセージおよび／または鍵材料を含むことが可能なアクセス受付けメッセージをＡＰ１５２４に送信することができる。ＥＡＰ成功メッセージは、１５１８でＵＥ１５２０に（例えばＣＭ１５２２に）転送することができる。ＵＥ１５２０のステータスは、１５１９でＡＰ１５２４において「許可」の状態になることができる。ＵＥ１５２０は、（例えばＤＨＣＰを使用して）ＩＰアドレスを取得し、ＡＰ１５２４を介してインターネットにアクセスすることができる。

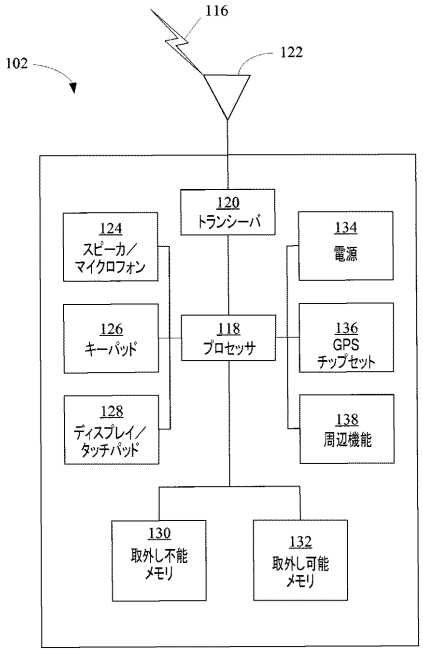
【０１７８】

上記では特定の組合せで特徴および要素について説明したが、当業者は、各特徴または要素は単独で、または他の特徴および要素との任意の組合せで使用可能であることを認識されよう。また、本明細書に記載の方法は、コンピュータまたはプロセッサによる実行のためにコンピュータ可読媒体に組み込まれた、コンピュータプログラム、ソフトウェア、またはファームウェアにて実装することができる。コンピュータ可読媒体の例は、電子信号（有線または無線接続を通じて伝送される）、およびコンピュータ可読記憶媒体を含む。コンピュータ可読記憶媒体の例は、これらに限定されないが、読み出し専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、レジスタ、キャッシュメモリ、半導体メモリ装置、内蔵ハードディスクや取外し可能ディスクなどの磁気媒体、光磁気媒体、およびＣＤ－ＲＯＭディスクやデジタル多用途ディスク（ＤＶＤ）などの光学媒体を含む。ソフトウェアと関連したプロセッサを使用して、ＷＴＲＵ、ＵＥ、端末、基地局、ＲＮＣ、または任意のホストコンピュータで使用するための無線周波トランシーバを実装することができる。

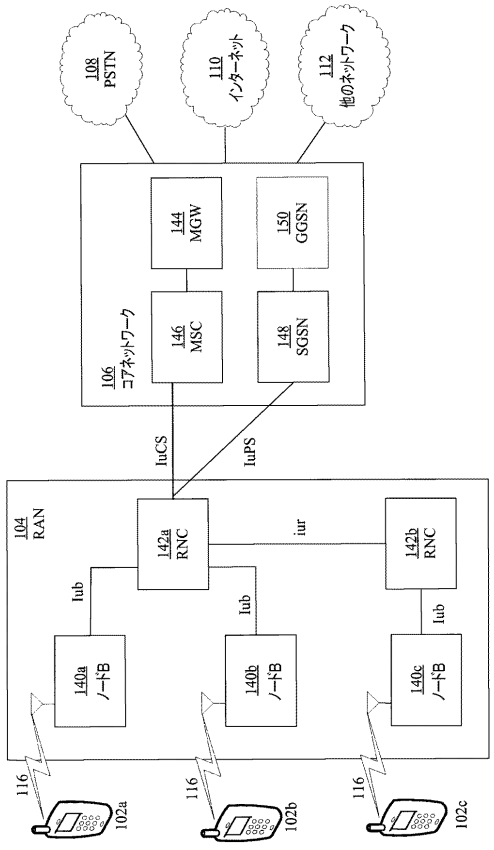
【図１Ａ】



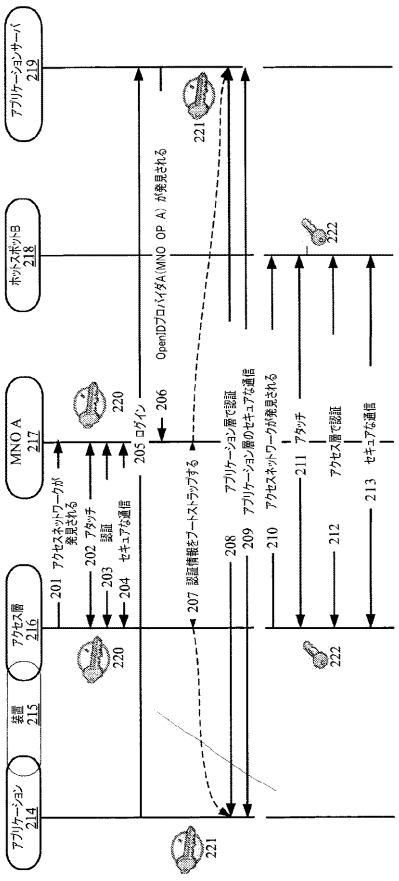
【図１Ｂ】



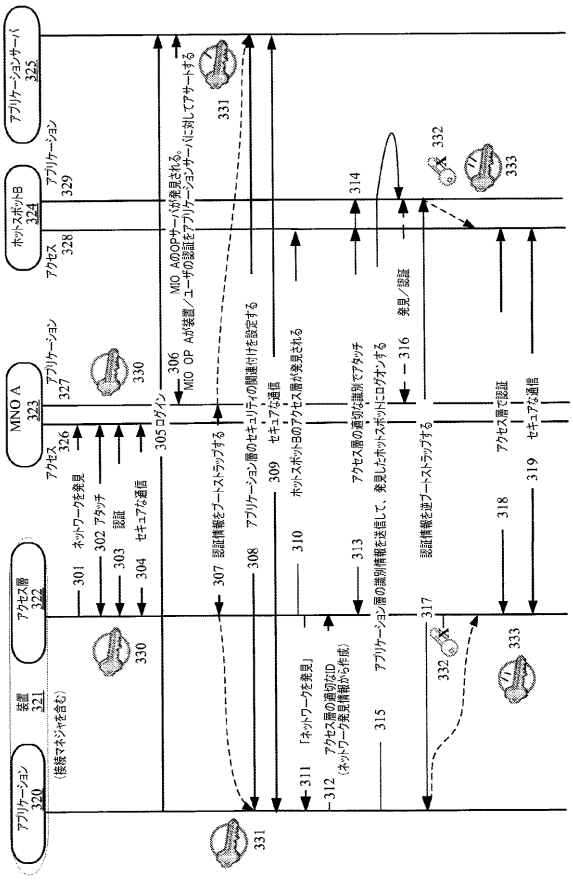
【図１Ｃ】



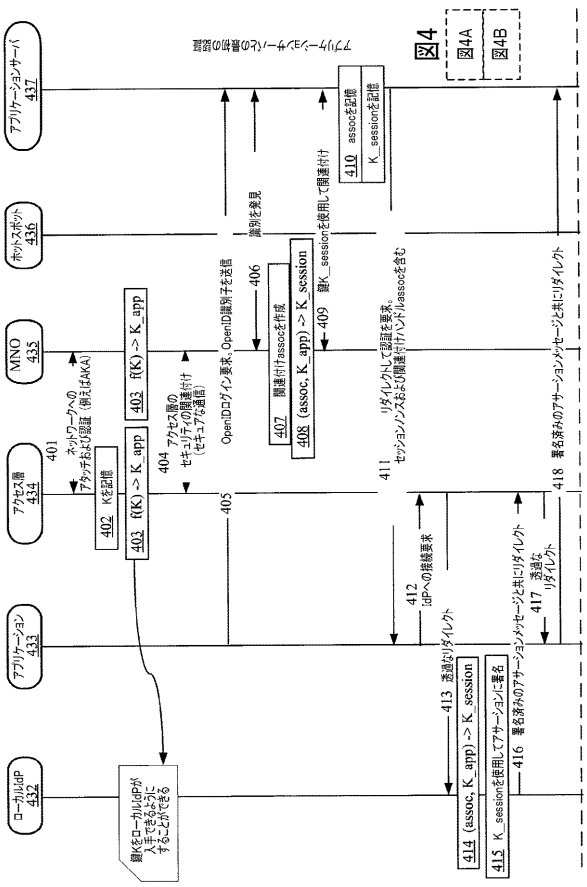
【図２】



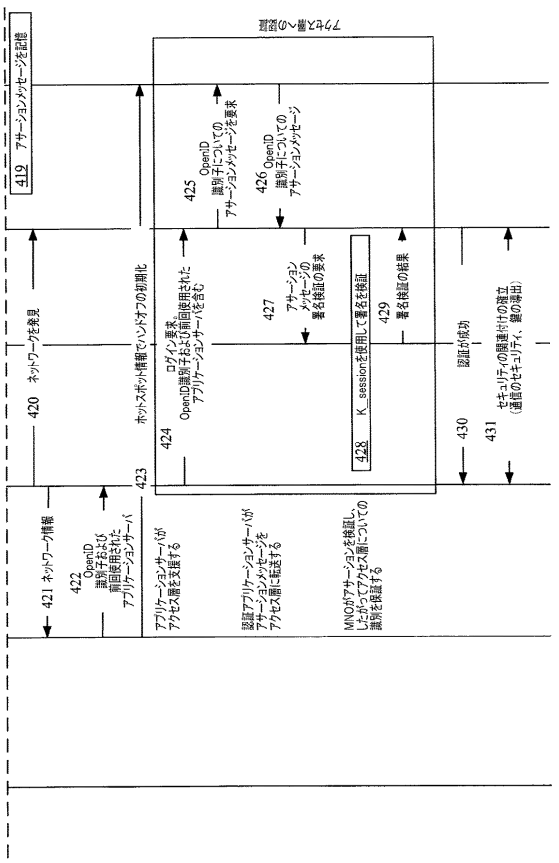
【図３】



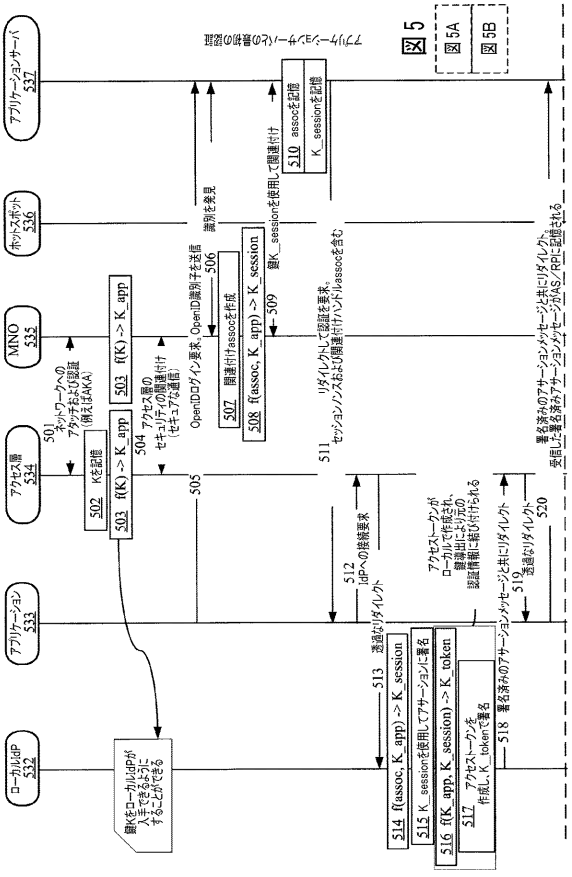
【図４Ａ】



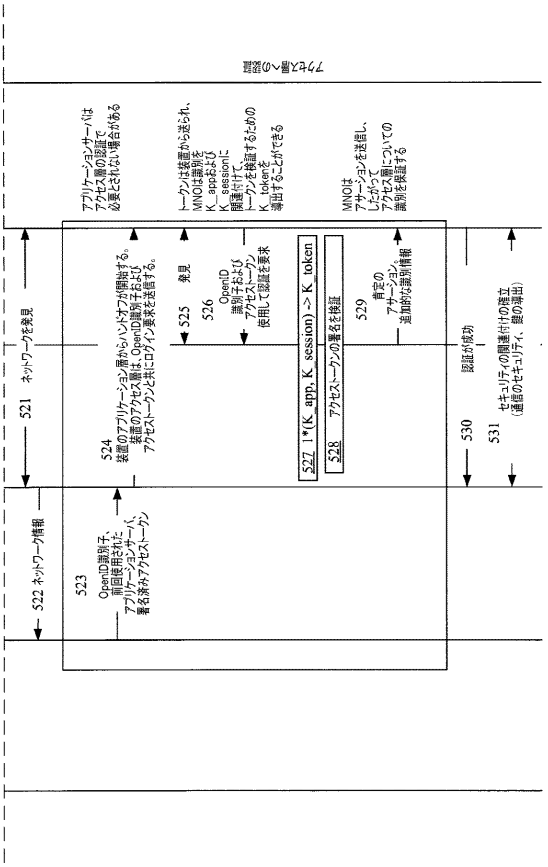
【図４Ｂ】



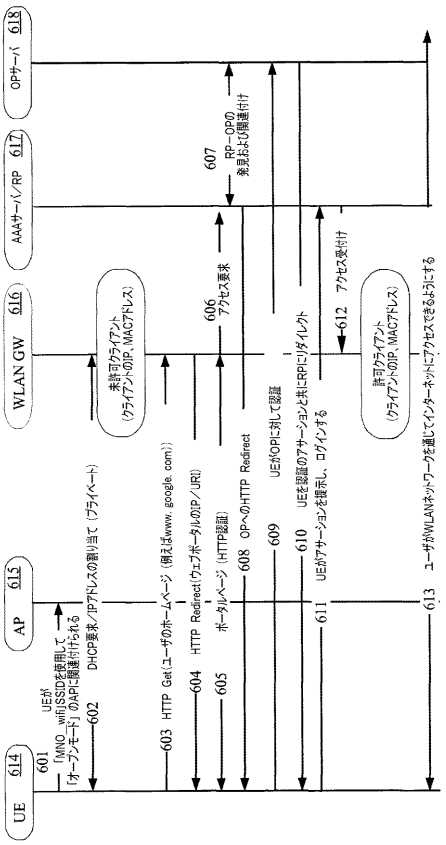
【図５Ａ】



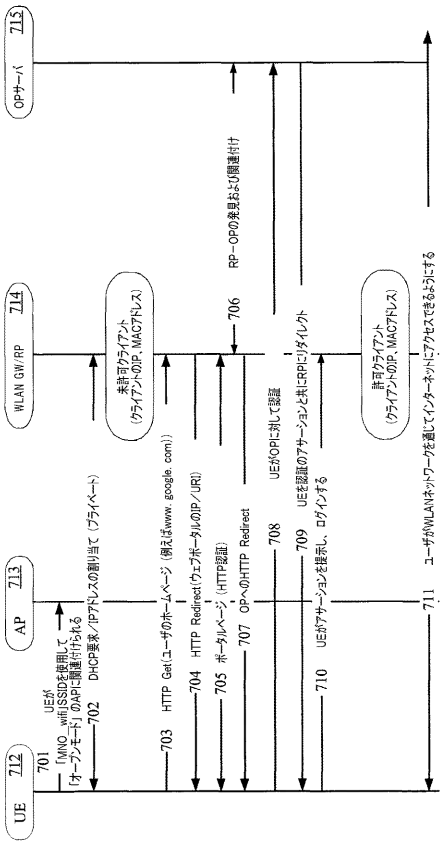
【図５Ｂ】


521 ネットワークを発見
522 ネットワーク情報
523 OpenID識別子、前回使用された アプリケーションサーバ、 署名済みアクセストークン
524 装置のアプリケーション層からハンドオフが開始する。 装置のアクセス層は、OpenID識別子および アクセストークンと共にログイン要求を送信する。
525 発見
526 OpenID 識別子および アクセストークン 使用して認証を要求
527 I*(K_app, K_session) -> K_token
528 アクセストークンの署名を検証
529 真正の アサーション 追加的な識別情報
530 認証が成功
531 セキュリティの関連付けの確立 (通信のセキュリティ、鍵の導出)
アプリケーションサーバは アクセス層の認証に 必要とされない場合がある
トークンは装置から送られ、 MNOは識別子 K_appおよび K_sessionに 関連付けて トークンを検証するための K_tokenを 導出することができる
MNOは アサーションを送信し、したがって アクセス層についての 識別を保証する
アプリケーション層 セッション層

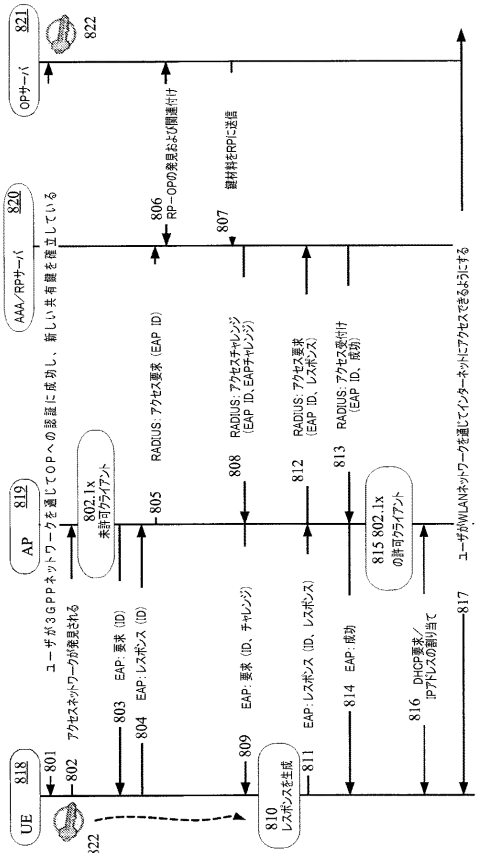
【図６】


UE 614
AP 615
WLAN GW 616
AAAサーバ/RP 617
OPサーバ 618
601 UEが「MNO_wifi」SSIDを使用して「オープンモード」のAPに関連付ける
602 DHCP要求/IPアドレスの割り当て（プライベート）
603 HTTP Get（ユーザのホームページ（例えばwww.google.com））
604 HTTP Redirect（ウェブポータルのIP/URI）
605 ポータルページ（HTTP認証）
606 アクセス要求
607 RP-OPの発見および関連付け
608 OPへのHTTP Redirect
609 UEがOPに対して認証
610 UEを認証のアサーションと共にRPにリダイレクト
611 UEがアサーションを提示し、ログインする
612 アクセス受付け
613 ユーザがWLANネットワークを通じてインターネットにアクセスできるようにする
未許可クライアント（クライアントのIP、MACアドレス）
許可クライアント（クライアントのIP、MACアドレス）

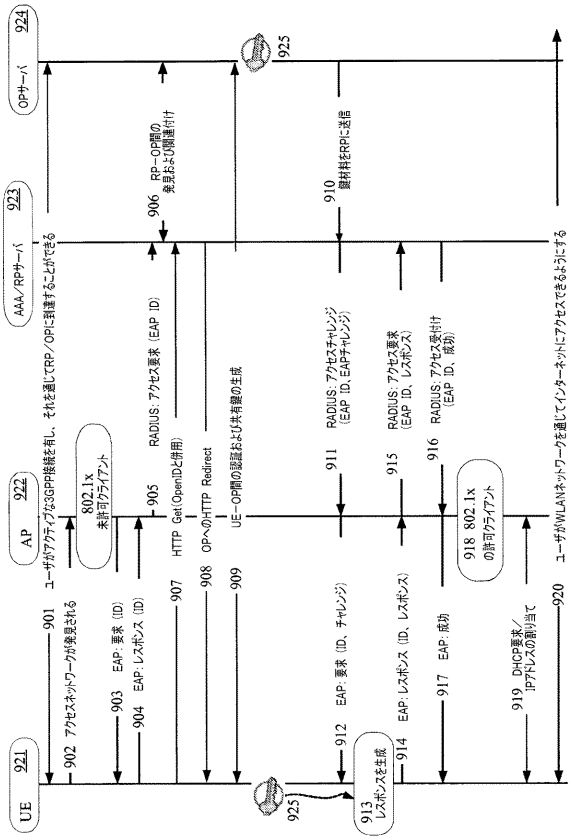
【図７】


UE 712
AP 713
WLAN GW/RP 714
OPサーバ 715
701 UEが「MNO_wifi」SSIDを使用して「オープンモード」のAPに関連付ける
702 DHCP要求/IPアドレスの割り当て（プライベート）
703 HTTP Get（ユーザのホームページ（例えばwww.google.com））
704 HTTP Redirect（ウェブポータルのIP/URI）
705 ポータルページ（HTTP認証）
706 RP-OPの発見および関連付け
707 OPへのHTTP Redirect
708 UEがOPに対して認証
709 UEを認証のアサーションと共にRPにリダイレクト
710 UEがアサーションを提示し、ログインする
711 ユーザがWLANネットワークを通じてインターネットにアクセスできるようにする
未許可クライアント（クライアントのIP、MACアドレス）
許可クライアント（クライアントのIP、MACアドレス）

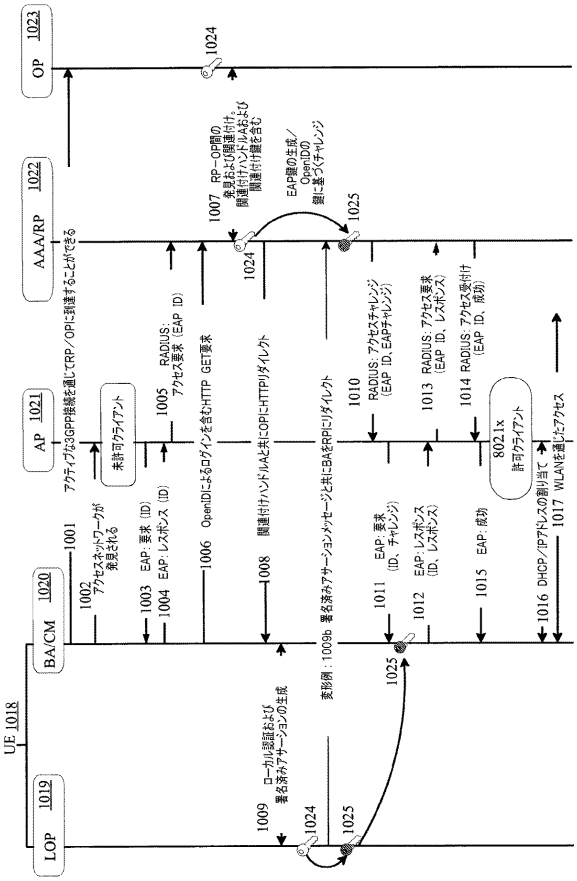
【図８】


UE 818
AP 819
AAA/RPサーバ 820
OPサーバ 821
801 ユーザが3GPPネットワークを通じてOPへの認証に成功し、新しい共有鍵を確立している
802 アクセスネットワークが発見される
803 EAP: 要求（ID）
804 EAP: レスポンス（ID）
805 RADIUS: アクセス要求（EAP ID）
806 RP-OPの発見および関連付け
807 資材料をRPに送信
808 RADIUS: アクセスチャレンジ（EAP ID, EAPチャレンジ）
809 EAP: 要求（ID、チャレンジ）
810 レスポンスを生成
811 EAP: レスポンス（ID、レスポンス）
812 RADIUS: アクセス要求（EAP ID、レスポンス）
813 RADIUS: アクセス受付け（EAP ID、成功）
814 EAP: 成功
815 802.1xの許可クライアント
816 DHCP要求/IPアドレスの割り当て
817 ユーザがWLANネットワークを通じてインターネットにアクセスできるようにする
822
802.1x 未許可クライアント

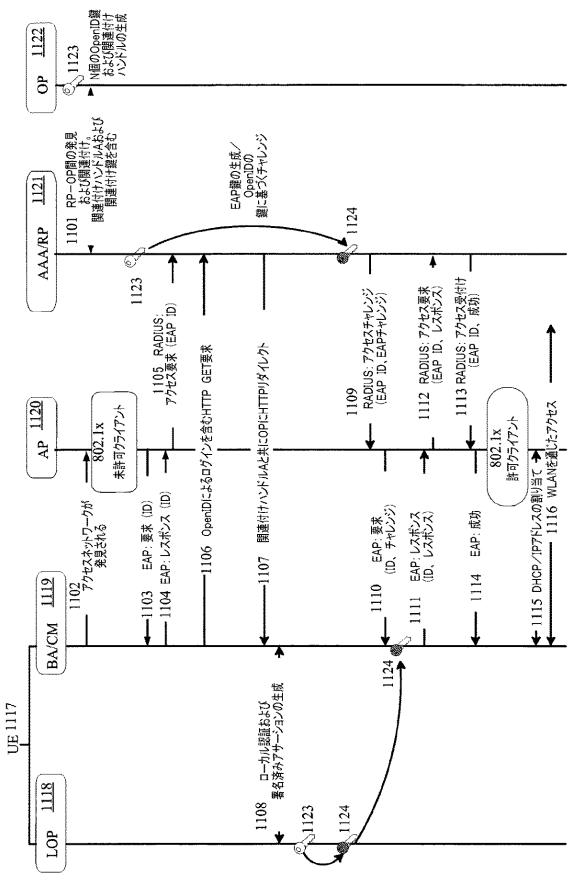
【図９】



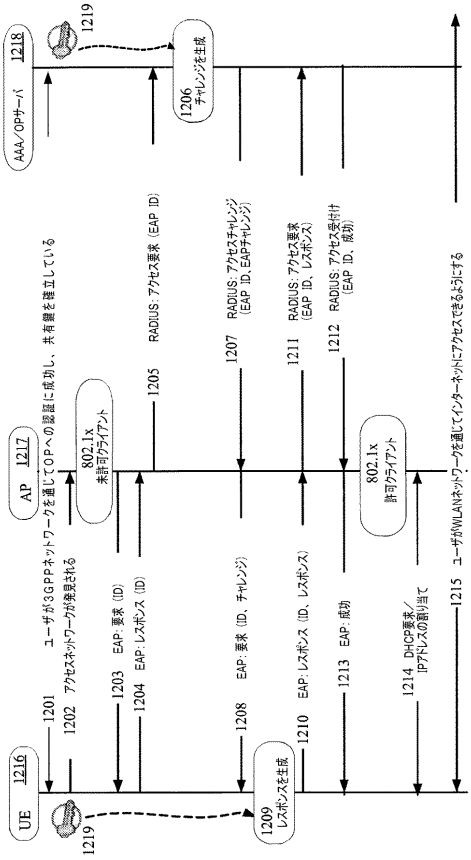
【図１０】



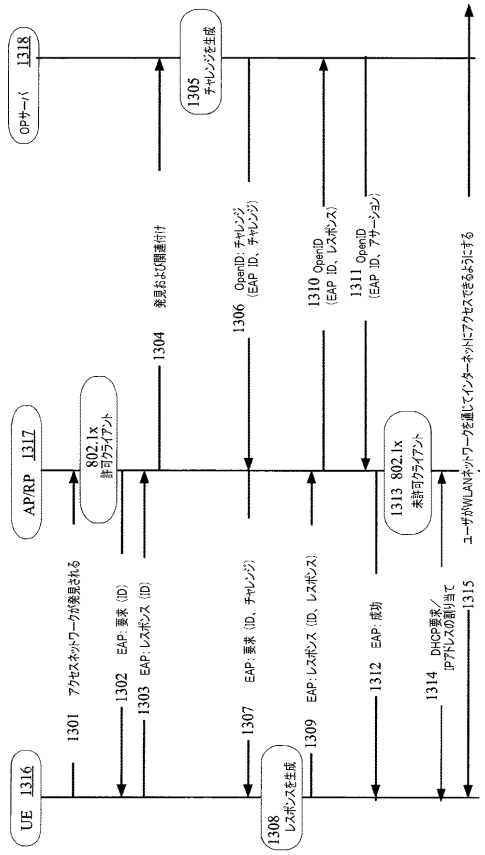
【図１１】



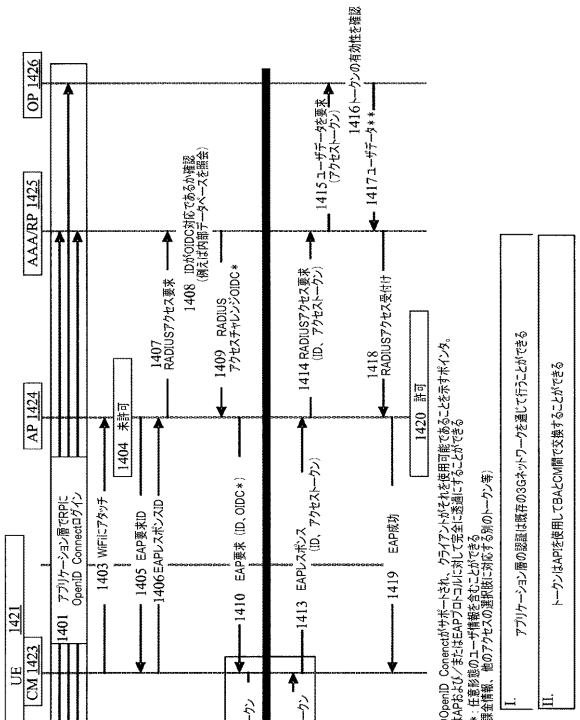
【図１２】



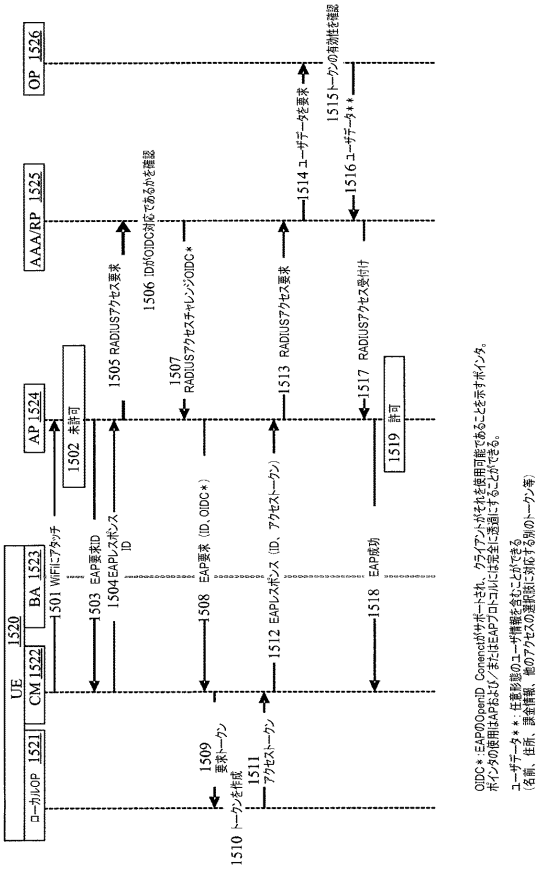
【図１３】


UE 1316
AP/RP 1317
OPサーバ 1318
1301 アクセスネットワークが発見される
802.1x 許可クライアント
1302 EAP: 要求 (ID)
1303 EAP: レスポンス (ID)
1304 発見および関連付け
1305 チャレンジを生成
1306 OpenID: チャレンジ (EAP ID、チャレンジ)
1307 EAP: 要求 (ID、チャレンジ)
1308 レスポンスを生成
1309 EAP: レスポンス (ID、レスポンス)
1310 OpenID (EAP ID、レスポンス)
1311 OpenID (EAP ID、アサーション)
1312 EAP: 成功
1313 802.1x 未許可クライアント
1314 DHCP要求／IPアドレスの割り当て
1315 ユーザがWLANネットワークを通じてインターネットにアクセスできるようにする

【図１４】


UE 1421
BA 1422
CM 1423
AP 1424
AAA/RP 1425
OP 1426
1401 アプリケーション層でRP(に OpenID Connectログイン
1402 アクセストークンを記憶
1403 WiFiにアタッチ
1404 未許可
1405 EAP要求ID
1406 EAPレスポンスID
1407 RADIUSアクセス要求
1408 IDがOIDC対応であるか確認 (例えば内部データベースを照会)
1409 RADIUS アクセスチャレンジOIDC*
1410 EAP要求 (ID、OIDC*)
1411 要求トークン
1412 アクセストークン
1413 EAPレスポンス (ID、アクセストークン)
1414 RADIUSアクセス要求 (ID、アクセストークン)
1415 ユーザデータ要求 (アクセストークン)
1416 トークンの有効性を確認
1417 ユーザデータ**
1418 RADIUSアクセス受付
1419 EAP成功
1420 許可
OIDC*: EAPのOpenID Connectがサポートされ、クライアントがそれを使用可能であることを示すポインタ。
ポインタの使用はAPおよび／またはEAPプロトコルに対して完全に透過にすることができる。
ユーザデータ**: 任意形態のユーザ情報を含むことができる。
(名前、住所、課金情報、他のアクセスの選択肢に対応する別のトークン等)
I. アプリケーション層の認証は既存の3Gネットワークを通じて行うことができる
II. トークンはAPを使用してEAPとCM間で交換することができる

【図１５】


UE 1520
ローカルOP 1521
CM 1522
BA 1523
AP 1524
AAA/RP 1525
OP 1526
1501 WiFiにアタッチ
1502 未許可
1503 EAP要求ID
1504 EAPレスポンス ID
1505 RADIUSアクセス要求
1506 IDがOIDC対応であるかを確認
1507 RADIUSアクセスチャレンジOIDC*
1508 EAP要求 (ID、OIDC*)
1509 要求トークン
1510 トークンを作成
1511 アクセストークン
1512 EAPレスポンス (ID、アクセストークン)
1513 RADIUSアクセス要求
1514 ユーザデータを要求
1515 トークンの有効性を確認
1516 ユーザデータ**
1517 RADIUSアクセス受付
1518 EAP成功
1519 許可
OIDC*: EAPのOpenID Connectがサポートされ、クライアントがそれを使用可能であることを示すポインタ。
ポインタの使用はAPおよび／またはEAPプロトコルに対して完全に透過にすることができる。
ユーザデータ**: 任意形態のユーザ情報を含むことができる。
(名前、住所、課金情報、他のアクセスの選択肢に対応する別のトークン等)

フロントページの続き

(51)Int.Cl.		FI		
H04W 80/02	***(2009.01)***	H04M	3/42	B
H04W 80/12	***(2009.01)***	H04W	80/02	
		H04W	80/12	

(72)発明者　インヒョク　チャ
大韓民国　ソウル　カンナムーク　サムスン　ドン　１４－１　ヨンーアン　ハイツ　ビレッジ　１０２－ドン　２０２－ホ
(72)発明者　アンドレアス　シュミット
ドイツ　６５９２９　フランクフルト　アム　マイン　チュートネンウェグ　３７
(72)発明者　ルイス　ジェイ．グッチョーネ
アメリカ合衆国　１０７０９　ニューヨーク州　イースト　チェスター　リンカーン　プレイス　２１１
(72)発明者　ローレンス　ケース
アメリカ合衆国　７８７３４　テキサス州　オースティン　ティモシー　サークル　５００２
(72)発明者　アンドレアス　レイチェル
ドイツ　６０３８５　フランクフルト　ハイデシュトラッセ　１３１
(72)発明者　ヨウシフ　タルガリ
アメリカ合衆国　０７７２１　ニュージャージー州　クリフウッド　デラウェア　アベニュー　１８３

審査官　桑原　聡一

(56)参考文献　Using the liberty alliance architecture to secure IP-level handovers, Communication System Software and Middleware, 2006. Comsware 2006. First International Conference on , IEEE, ２００６年, ＵＲＬ, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1665154

(58)調査した分野(Int.Cl., ＤＢ名)

Ｈ０４Ｂ	７／２４－７／２６
Ｈ０４Ｗ	４／００－９９／００
Ｈ０４Ｍ	３／００
Ｈ０４Ｍ	３／４２